

ALTO 818

ACCESS CONTROL UNITS

SE 818SC and SE 818SX

INSTALLATION and

OPERATION

MANUAL



**Westinghouse
Security Electronics**

an ISO 9001 certified company

5452 Betsy Ross Drive
Santa Clara, CA 95054-1184
408-727-5170
Fax 408-727-6707
P/N 66109074001, Rev. D

© Copyright 1997 Westinghouse Security Electronics.
All rights reserved. Printed in the United States of America.
DuraKey™, QuadraKey™, NexKey™, NexSentry™ and DigiReader™ are trademarks of
Westinghouse Security Electronics.

Limited Warranty

Westinghouse Security Electronics warrants to the original user the Equipment manufactured by Security Electronics as described herein (the Equipment) to be free from defects in material and workmanship for a period of one year from the date of purchase by such user or fifteen (15) months from the date of shipment from the factory, whichever is sooner, provided:

- I Security Electronics has been notified within such period by return of any alleged defective equipment, free and clear of any liens and encumbrances to Security Electronics or its authorized Dealer at the address specified, transportation prepaid; and
- II the Equipment has not been abused, misused or improperly maintained and/or repaired during such period; and
- III such defect has not been caused by ordinary wear and tear; and
- IV such defect is not a result of voltage surges/brownouts, lightning, water damage/flooding, fire, explosion, earthquakes, tornadoes, acts of aggression/war or similar phenomena; and
- V accessories used as an integral to Security Electronics Systems have been approved by Security Electronics (e.g., coaxial cables, batteries, etc.); and
- VI the Equipment has been installed, the installation supervised or installation tested by an authorized Security Electronics Dealer.

Command Keys are warranted for 5 years. Security Electronics shall at its option, either repair or replace, free of charge, the Equipment found, upon Security Electronics' inspection to be so defective, or if agreed upon, refund the purchase price, less a reasonable allowance for depreciation, in exchange for the Equipment. Magnetic Stripe Cards are warranted as described by the manufacturer's warranty.

SECURITY ELECTRONICS MAKES NO OTHER WARRANTY, AND ALL IMPLIED WARRANTIES INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE EXPRESSED WARRANTY PERIOD AS SET FORTH ABOVE.

SECURITY ELECTRONICS MAXIMUM LIABILITY HEREUNDER IS LIMITED TO THE PURCHASE PRICE OF THE EQUIPMENT. IN NO EVENT SHALL SECURITY ELECTRONICS BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL OR SPECIAL DAMAGES OF ANY NATURE ARISING FROM THE SALE OR USE OF THE PRODUCT.

Some states do not allow limitations on incidental or consequential damages or how long an implied warranty lasts, so the above limitations may not apply. This warranty gives specific legal rights; however, other rights which vary from state to state, may pertain.

The information provided in this manual is believed to be accurate and reliable. However, Westinghouse Security Electronics (WSE) assumes no responsibility for any errors that may appear. Possession of this manual does not imply the granting of licenses to make or sell equipment or software constructed according to descriptions provided.

FEDERAL COMMUNICATIONS COMMISSION RADIO FREQUENCY INTERFERENCE STATEMENT

Alto 818 access control units manufactured by Westinghouse Security Electronics have been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions herein, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Insure that this equipment is not connected to the same AC power outlet as the receiver.
- Consult the dealer or an experienced radio/TV technician for help.



Listed
56Z7

UL 294 ACCESS CONTROL SYSTEM

The SE 818SC and SE 818SX are UL 294 listed. Installation according to this manual will meet specifications for a UL 294 access control system.

Contents

List of Figures	xi
List of Tables	xiii

Section 1: Introduction

1.1	Manual Conventions	1-2
1.2	System Features	1-3
1.2.1	Access Control	1-4
1.2.2	System S-, E-, and H-Mode Operation	1-4
1.2.3	Monitoring	1-4
1.2.4	System Test	1-4
1.3	Principles of Operation	1-5
1.3.1	Users and Card holders	1-5
1.3.2	Building Modes	1-5
	Building Open Mode	1-6
	Building Limited Mode	1-6
	Building Closed Mode	1-6
	Changing Building Modes	1-6
1.3.3	Sensor Types	1-7
	Normal Sensor	1-7
	Open Sensor	1-7
	Closed Sensor	1-7
	Station Sensor	1-7
1.3.4	Privileged Versus Non-Privileged Card Holders	1-7
1.3.5	Door Control	1-8
	Door Locks	1-8
	Door Switches	1-9
	Request-to-Exit	1-9
1.3.6	Anti-Passback	1-9
	Hard Anti-Passback	1-10
	Soft Anti-Passback	1-10
	REX and DS Considerations	1-10
	Anti-Passback Status	1-10
	Typical Anti-Passback Installation	1-10
1.3.7	Remote Station	1-11
1.3.8	Tamper Switches	1-11
1.3.9	Duress Code	1-12

Section 2: System Description

2.1	Alto 818 Access Control Unit	2-4
2.1.1	Electronics	2-5
	Lithium Battery	2-5
	Main PCA Switches	2-6
	LED Panel	2-6
	MSM Auto Sensing PCA	2-7
2.1.2	ACU System Interface	2-7
	Power (P1)	2-7
	Relays	2-8
	20 mA	2-8
	Host	2-8
	Terminal	2-9
	Annunciator	2-9
	RS-485	2-9
	Sensors	2-9
2.2	Power Modules	2-10
2.2.1	SE 3708CU / SE 3718SU Power Modules with Backup Batteries	2-10
2.2.2	SE 3018S/ SE 3018-2 Power Modules	2-12
2.2.3	SE 3708C Power Module with Backup Batteries	2-13
2.2.4	Alarm-Saf Power Supply/Battery Charger Model AS/PS5-BFS-24-UL	2-13
	LED Indicators	2-13
	Fuses	2-14
	Backup Batteries	2-14
	Power Supply/Battery Enclosure	2-15
2.2.5	Power Inserter	2-15
2.3	Terminal, Host and Printer	2-16
2.3.1	Terminal	2-16
2.3.2	Host Computer	2-16
2.3.3	Printer	2-16
2.4	SE 778-A Annunciator/Control Module	2-17
2.4.1	Latched Contacts and Indicator	2-18
2.4.2	Control Contacts and Indicators	2-18
2.4.3	Station Switch and Indicators	2-18
2.4.4	Remote Station	2-19
2.5	SE 774-A Multiple Switch Monitor (MSM)	2-20
2.6	Communication Interfaces	2-22
2.6.1	CI-1 Communications Interface	2-22
2.6.2	CI-8 Communications Interface	2-23
2.7	Analog Proximity Sensors	2-24
2.7.1	Proximity Sensor Operation	2-24
2.7.2	Proximity Sensor Models	2-24
	SE 2814/15 Proximity Sensors	2-24
	SE 2854/55 Medium Range Sensor	2-25
	SE 2804 Compact Sensor	2-25

2.8	DigiReader Digital Command Key Readers	2-27
2.9	VIP2 Keypad	2-28
2.9.1	Keypad Used with a Sensor	2-29
2.9.2	VIP2 in Stand-Alone Operation	2-29
2.9.3	VIP2 LEDs	2-29
2.9.4	Duress Code Feature	2-29
2.10	Modems	2-30
2.11	NexStar RS-485 Multiplexer	2-31
2.12	S-Net	2-32
2.13	Door Control Configurations	2-33
2.13.1	One-Reader Control	2-33
2.13.2	Two-Reader Control	2-34
2.14	System Modes	2-35
2.14.1	Operate Mode	2-35
2.14.2	Command Mode	2-35

Section 3: Installation Planning

3.1	Installation Planning	3-2
3.1.1	Safety Precautions	3-2
3.1.2	Plan Procedures	3-3
3.2	Environmental Requirements	3-5
3.3	Hardware Location	3-6
3.3.1	Alto 818 Controller	3-6
3.3.2	Analog Proximity Reader	3-6
3.3.3	DigiReader	3-8
3.3.4	Remote Station Switch	3-8
3.4	General Wiring Requirements	3-9
3.5	Coaxial Cable Installation	3-10
3.6	S-Net	3-11
3.6.1	Cable Losses	3-11
3.6.2	S-Net Power Wire Size	3-12
3.6.3	Alternatives to Large Power Wire	3-13
3.6.4	Future System Expansion	3-13
3.6.5	S-Net Cable	3-13
3.6.6	Termination Resistors	3-14
3.6.7	NexStar RS-485 Multiplexer	3-14
3.6.8	Wire Insertion	3-15
3.7	S-Net Power Requirements	3-16
3.8	Alto 818 Mounting	3-17
3.9	Controlled Doors	3-18
3.9.1	Unmonitored Doors	3-18
3.9.2	Door Locks	3-18
3.10	Multiple Switch Monitors	3-19
3.11	Monitored Inputs	3-20
3.12	Installation Sequence	3-21

Section 4: Wiring

4.1	AC Power	4-2
4.1.1	Grounding	4-2
4.1.2	ACU Connection	4-2
4.2	DC Power	4-4
4.2.1	Alarm-Saf Model AS/PS5-BFS-24-UL	4-4
	Single Alarm-Saf Installation	4-5
	Multiple Alarm-Saf Power Supplies Installation	4-5
4.2.2	Power Inserter	4-6
	Single Power Inserter Installation	4-7
	Multiple Power Inserters Installation	4-8
4.3	RS-485 Interface	4-9
4.4	Analog Sensors	4-11
4.5	Lock Wiring Interface	4-12
4.6	SE 744-A MSM Interface Wiring	4-13
4.6.1	Reader Connections	4-13
4.6.2	Monitor Point Connections	4-13
4.7	Host and System Terminal Interface Wiring	4-15
4.8	Remote Terminal Wiring	4-17
4.9	SE 778-A Interface Wiring	4-18
4.10	20 mA Loop Wiring	4-19
4.11	Remote Dial-Up Interface	4-20

Section 5: Bench Check

5.1	Unpacking	5-2
5.2	Test Setup	5-3
5.3	Test Procedures	5-6
5.3.1	Power On	5-6
5.3.2	Terminal Test	5-7
5.3.3	Lock Relay Test	5-8
5.3.4	Monitor Input Test	5-9
5.3.5	Sensor Test	5-10
5.3.6	RS-485 (S-Net) Test	5-10
	DigiReader	5-10
	VIP2	5-11
5.3.7	Bench Check Conclusion	5-12

Section 6: Commands

6.1	Keyboard Entries	6-2
6.1.1	Days and Dates	6-2
6.1.2	Time Entries	6-3
6.1.3	Enter Key	6-4
6.1.4	Escape (ESC) Key	6-4
6.2	Command Types	6-5

6.3	Command Descriptions	6-6
6.3.1	ACCESS	6-7
6.3.2	BYE	6-8
6.3.3	CLOSE	6-8
6.3.4	DELETE	6-9
6.3.5	DOOR	6-9
6.3.6	FORGIVE	6-16
6.3.7	GROUP	6-16
6.3.8	HELP	6-17
6.3.9	HOLIDAY	6-17
6.3.10	KEY	6-18
6.3.11	LIMIT	6-21
6.3.12	MODEM	6-21
6.3.13	MONITOR	6-23
6.3.14	OPEN	6-24
6.3.15	RELOCK	6-24
6.3.16	REPORT	6-24
6.3.17	RESET	6-26
6.3.18	SHUNT	6-26
6.3.19	SILENCE	6-27
6.3.20	STATUS	6-28
6.3.21	SYSTEM	6-29
6.3.22	TIME	6-34
6.3.23	UNLOCK	6-35
6.3.24	UNSHUNT	6-36
6.3.25	USER	6-36
6.3.26	VERSION	6-37
6.3.27	XLOAD	6-37
6.3.28	XSAVE	6-38

Section 7: Database Setup

7.1	Overview	7-2
7.1.1	System Administrator	7-2
7.1.2	User Authorization Rank	7-2
7.1.3	Default Database Parameters	7-3
	Default Password NEW	7-3
	Default Access Code 1	7-3
	Default Report 1	7-4
7.2	Preparation for Setup	7-5
7.2.1	Talk to the Owner	7-5
7.2.2	Command Keys	7-5
7.2.3	Listing Card holders	7-6
	Card Holder Names	7-7
	Access Codes	7-7
7.2.4	Listing Access Codes	7-7

7.2.5	Reports	7-7
	Log Events	7-7
	Report Actions	7-9
7.2.6	List of Doors	7-10
7.3	Creating the Database	7-11
7.3.1	Entering the Command Mode	7-11
7.3.2	Exiting the Command Mode	7-11
7.3.3	Command Sequence	7-12
7.3.4	PRINT Command	7-12

Section 8: Operation

8.1	Overview	8-2
8.2	Initial Power-On	8-3
8.3	Terminal Set-Up	8-4
8.4	Initial Log On	8-5
8.5	Operate Mode	8-6
8.6	Operator Responsibilities	8-7
8.6.1	System Monitoring	8-7
8.6.2	Response to Alarms	8-8
8.7	Operation Commands	8-9
8.7.1	CLOSE	8-9
8.7.2	FORGIVE	8-9
8.7.3	LIMIT	8-9
8.7.4	OPEN	8-10
8.7.5	RELOCK	8-10
8.7.6	SHUNT	8-10
8.7.7	SILENCE	8-10
8.7.8	STATUS	8-10
8.7.9	UNLOCK	8-11
8.7.10	UNSHUNT	8-11

Section 9: Annual Test for UL 294 System

Appendix A: Specifications

Appendix B: Database Setup Sheets

Appendix C: Coaxial Cable Vendors

Appendix D: Command Keys

Index

List of Figures

Figure	Description	Page
1-1	Anti-Passback Installation	1-11
2-1	Example Alto 818 System Block Diagram	2-3
2-2	Alto 818 Access Control Unit	2-4
2-3	Alto 818 Battery and Switch Locations	2-5
2-4	Door Lock Circuitry Block Diagram	2-8
2-5	SE 3708CU Power Module with Backup Batteries and Enclosure	2-11
2-6	SE 3718SU Power Module with Backup Batteries and Enclosure	2-12
2-7	Model AS/PS5-BFS-24-UP Alarm Saf Power Supply/Battery Charger Wiring	2-14
2-8	SE 778-A Annunciator/Control Module	2-17
2-9	SE 774-A Multiple Switch Monitor (MSM)	2-20
2-10	CI-1 Installation Example	2-22
2-11	CI-8 Installation Example	2-23
2-12	VIP2 Keypad	2-28
2-13	S-Net Using a NexStar	2-31
2-14	S-Net Wiring	2-32
2-15	Example of One-Reader Door Control Configuration	2-33
2-16	Example of Two-Reader Door Control Configuration	2-34
3-1	Drop Wiring	3-14
3-2	S-Net Termination	3-15
3-3	Wire Insertion	3-15
4-1	SE 3708CU or SE 3718SU Power Module	4-3
4-2	Single Alarm-Saf Power Supply Installation	4-4
4-3	Multiple Alarm-Saf Power Supplies Installation	4-5
4-4	Power Inserter End View	4-6
4-5	Single Power Inserter to S-Net Wiring	4-7
4-6	Additional Power Inserter Wiring	4-8
4-7	RS-485 Interface Wiring for S-Net Devices and Tamper	4-9
4-8	Analog Proximity Sensors	4-11
4-9	Door Lock Interface Wiring	4-12
4-10	MSM Connections for N/O and N/C Monitoring Contacts	4-14
4-11	Host and Terminal RS-232C Interface Wiring Using a Null Modem Cable	4-15
4-12	SE 6000 System HP Terminal Concentrator Interface	4-16
4-13	Remote Terminal Interface Wiring	4-17
4-14	SE 778-A Annunciator/Control Panel Interface	4-18
4-15	20 mA Interface Wiring	4-19
4-16	Remote Dial-Up Interface Installation	4-20
5-1	MSM Configured for Bench Check	5-3
5-2	Alto 818 Test Setup	5-4
5-3	Alto 818 Switch Locations	5-7
5-4	Measuring Lock Relay Resistance	5-8

Figure	Description	Page
5-5	STATUS Display — Monitor Point 1.2 Active	5-9
5-6	STATUS Display — Sensor, DigiReader and VIP2	5-11
6-1	ACCESS Command Prompts	6-7
6-2	DOOR Command Prompts	6-10
6-3	GROUP Command Prompts	6-16
6-4	HOLIDAY Command Prompts	6-17
6-5	KEY Command Prompts	6-18
6-6	Command Key Code Number	6-19
6-7	PRINT KEY Screen with Resulting Output	6-21
6-8	MODEM Command Prompts	6-22
6-9	MONITOR Command Prompts	6-23
6-10	REPORT Command Prompts	6-25
6-11	Example of STATUS Display	6-28
6-12	SYSTEM Command Prompts	6-31
6-13	USER Command Prompts	6-36
8-1	Terminal Display Example	8-7
D-1	Analog Command Key Number	D-1
D-2	Digital Command Keys	D-2

List of Tables

Table	Description	Page
1-1	SE 818SC and SE 818SX Differences	1-3
1-2	Alto 818 Features	1-3
1-3	Privileged/Non-Privileged Access	1-8
2-1	WSE Alto 818 Compatible Products	2-2
2-2	Alto 818 System Interface Connectors	2-7
2-3	Recommended Power Module Backup Batteries	2-10
2-4	Alarm-Saf Specifications	2-13
2-5	Alarm-Saf Power Supply LED Indicators	2-14
2-6	Coaxial Cable Length/Maximum Read Range	2-25
2-7	SE 2804 Wiring	2-26
2-8	DigiReader Digital Command Key Readers	2-27
2-9	Short-Haul Modem versus Long-Haul Modem	2-30
3-1	Installation Site Product List	3-4
3-2	Environmental Requirements for WSE Products	3-5
3-3	S-Net Cable Recommendations	3-11
3-4	S-Net Typical Wire Loss (18 AWG)	3-11
3-5	S-Net Device Load	3-12
3-6	Power Wire Size	3-12
3-7	S-Net Device Supply Requirements	3-16
4-1	Power Inserter Pin-Outs	4-7
6-1	Command Categories	6-5
6-2	Command Ranks	6-6
7-1	Selectable Reports	7-8
D-1	Command Key Identification	D-2
D-2	Digital Command Key Specifications	D-3
D-3	Digital Command Key Read Ranges	D-3

SECTION 1: INTRODUCTION

The Alto 818 access control units, SE 818SC and SE 818SX, are central processing devices for access control and alarm monitoring systems manufactured by Westinghouse Security Electronics (WSE). These systems comprise the ACU and associated hardware, either manufactured or supplied by WSE, required to configure an access control and monitoring installation of up to eight doors.

- The SE 818SC and SE 818SX are listed by Underwriters Laboratories and meet Access Control Standard ANSI/UL 294 when installed according to the instructions in this manual.
- All system installation wiring must be in accordance with the National Electrical Code ANSI/NFPA70.
- The SE 818SC and SE 818SX are not intended to be used as a burglar or fire alarm system and shall not be used where the local authority having jurisdiction requires a UL-Listed burglar alarm system.

The purpose of this manual is to provide the information for installing and using the SE 818SC and SE 818SX. This includes developing an installation plan and installing all hardware items. Database setup and system operation are discussed in Sections 7 and 8.

Each installation plan is tailored to the particular requirements of the building or area the system is designed to protect taking into account the capabilities of the hardware items available to implement these requirements. Consequently, the type and quantity of system hardware items required for a specific application cannot be specified here. This manual is limited to descriptions of the hardware items available for all applications, instructions for developing an installation plan, and guidelines for proper installation.

This manual is written for installations in which the ACU is functioning as a stand-alone access control system, S-mode (see Section 1.2.2). Installations in which the ACU is reporting to and controlled by a security management system such as the SE 5850 or the SE 6000, E-mode, are covered in detail in the SE 5850 and SE 6000 technical manuals.

The information provided in this manual is not intended to conflict with the specific building codes, electrical codes, fire codes, or safety codes to which any given system design must conform.

1.1 MANUAL CONVENTIONS

In addition to the basic information given in this manual, there are notes, cautions and warnings. These are defined and displayed within the manual as shown below.

NOTE:

A reminder or cross-reference to information or instruction located elsewhere in the manual. A note may also be a hint for ease of use.

CAUTION:

A caution indicates that failure to follow the supplied instructions or information may result in loss of data or damage to hardware.

WARNING:

A WARNING MEANS THAT FAILURE TO FOLLOW INSTRUCTIONS OR INFORMATION MAY RESULT IN INJURY TO PERSONNEL.

1.2 SYSTEM FEATURES

The SE 818SC and SE 818SX comprise the Alto 818 ACUs. Table 1-1 indicates the basic differences between the two models. Specific differences will be indicated, where appropriate throughout this manual.

Table 1-1: SE 818SC and SE 818SX Differences

	SE 818SC	SE 818SX
Supports SE 2854/55 Analog Sensors	No	Yes
Supports S-Net Digital Readers and Smart Card Readers (AT&T product)	Yes	No

The access control and monitoring features of the Alto 818 ACU are listed in Table 1-2.

Table 1-2: Alto 818 Features

Access Control Features	
Reader inputs	8
Maximum command keys	2,000 with numbers and names in H-mode; 5,200 with numbers only 4,400 with numbers and names in E- and S-modes; 11,200 with numbers only
Maximum access codes	15 in H-mode, 120 in E or S-modes
User-defined holidays	Up to 30
User-defined reports	Up to 32
Authorization levels	6
Individual operator IDs	8
Event log capacity	100 in H-mode; 4,000 in E- and S-modes
Monitoring Features	
Monitored input points (using SE 774A Multiple Switch Monitors)	Up to 32 plus power fail and tamper
Output contacts (includes SE 788-A control contacts)	Up to 16
Controlled entrances	Up to 8
Operating modes	Open, Limited and Closed

1.2.1 ACCESS CONTROL

A combination of proximity readers and keypads can be used to control entry to a building or controlled area. With proximity sensors a key holder places a command key close to a reader mounted near a controlled door. The command key is detected and its coded information is transmitted back to the Alto 818. Access is granted only when the key is valid and other pre-programmed criteria are matched. Similarly, when a personal identification number (PIN) is entered on a keypad, access is granted when the preprogrammed criteria are met.

The Alto 818 can provide a complete log of all keys presented, all PINs entered and all locks it has operated. An operator can take action based on the log to override the database software to open or close door locks or modify the system response to monitored activities.

1.2.2 SYSTEM S-, E-, AND H-MODE OPERATION

The Alto 818 is a stand-alone access control system that can also report to and be controlled by a remote host computer. When the Alto 818 is operating as a stand-alone system, it is operating in the S-Mode.

When the Alto 818 is connected to a WSE host such as the WSE SE 5850 or SE 6000 security management system, communication is via Security Electronics Extended Protocol (SEEP). In this instance, the Alto 818 is said to be operating in the E-mode.

When the Alto 818 reports to and is controlled by any other host, it is operating in the H-mode.

1.2.3 MONITORING

Door switches that detect door openings and other monitor points throughout the building or access control area are constantly monitored for a change in state.

1.2.4 SYSTEM TEST

While in operation, the Alto 818 is in a constant process of system test. If a fault occurs, a message identifying the fault will be displayed and printed in the system log. If an uninterruptible power supply is used with the system and the system is being powered by the backup batteries, a fault message can be generated when the battery charge level becomes low. The database can be set up to send such fault messages to a host or terminal, to prevent closure of the building, to send a message over a dial-up modem, and to trigger an alarm device.

1.3 PRINCIPLES OF OPERATION

This section describes terms and principles which are specific to access control systems. They are provided here for those who are not experienced with other WSE ACUs such as the SE 422. This section is not intended as a complete glossary, but to familiarize the reader with words and concepts used throughout the manual.

1.3.1 USERS AND CARD HOLDERS

The term user is equivalent to system operator. The Alto 818 allows eight levels of users to be defined. The person with overall responsibility for the database setup and control of the system functions will be assigned the rank of A, with access to all systems commands. Other ranks may be assigned to security personnel who will not need any setup commands but will use only operation commands. Another rank may be specified for use by Human Resources or security staff responsible for maintaining information and access properties of all card holders.

A card holder is an individual who has a digital or analog command key which has been defined in the Alto 818 database with the KEY command. Many references to card holders are also valid for individuals who use a keypad only.

1.3.2 BUILDING MODES

The Alto 818 can be configured to recognize three building modes: Open, limited and closed. The access control system can function differently in each mode. These differences include:

- The ability of the system to ignore or react to system activity such as doors forced open, doors held open too long, access events, and monitor point activity.
- The ability to deny access to some or all card holders regardless of their access codes depending on the sensor type to which their cards were presented.

The advantages of using building modes depend upon the access control requirements of a particular installation. In installations that have regularly scheduled hours of activity, building modes simplify the access control process. For buildings in which a significant number of employees work flexible schedules, or whose work requires them to come and go at irregular hours, defining building modes may not be desirable.

The three building modes are defined below.

BUILDING OPEN MODE

The building open mode is used during periods of time such as normal working hours when access to buildings or controlled areas needs to be authorized for the greatest number of card holders. Door switches and monitor points that trigger alarms in the building limited or closed mode can be set to remain silent during the building open mode.

BUILDING LIMITED MODE

The building limited mode is used during periods of time in which only part of the building or area is to be empty and only some of its monitor inputs are to be active. During this mode, areas in which security requirements are minimal would be made accessible to card holders such as janitorial personnel, etc., while doors to more sensitive areas would be locked and their monitor points would trigger alarms.

BUILDING CLOSED MODE

The building closed mode is used when the building is unoccupied. Door switches and monitor points that do not trigger alarms in open or limited mode can be defined to do so in the closed mode. Authorized access to buildings or controlled areas will be minimal. The individual who places the system in the building closed mode must first ensure that everyone else has left the building. Anyone still in the building when it was closed could set off an alarm when leaving the building or be locked in, depending upon the type of door locks used.

CHANGING BUILDING MODES

Building modes can be changed by two methods:

- From the system terminal by an operator assigned rank D or higher through the use of the OPEN, LIMIT, or CLOSE commands.
- From a remote station switch by a privileged (see Section 1.3.4) card holder who has access to the switch. Limited mode cannot be selected by this method. For security purposes, the remote switch should be restricted in its use to only a few individuals by making it a key switch.

The Alto 818 will refuse to change the building mode from open to either limited or closed if any report event is active which is programmed through the REPORT command to prevent building closure. A log message will be sent to the terminal and host ports that an attempt was made to change the building mode and will identify the problem. After the problem has been corrected the building mode can be changed.

System operators can use the STATUS command to identify any pending activity that can prevent building closure. The problem can then be fixed or the SHUNT command can be used to override the activity and the building mode can then be changed.

1.3.3 SENSOR TYPES

The DOOR command is used to assign a sensor type to devices when building modes are to be used. Each sensor is defined as normal, open, closed or as a station sensor. If building modes are not used, all sensors act as a normal sensors.

NORMAL SENSOR

A normal sensor grants access during all building modes to card holders who present a card key during a valid time interval on a day specified for their access code.

OPEN SENSOR

An open sensor grants access only during the building open mode. Access is denied to all, including privileged card holders, during the limited and closed modes.

CLOSED SENSOR

A closed sensor grants access during the open mode if a valid card is presented. In limited and closed modes, access is granted to privileged card holders only.

STATION SENSOR

A station sensor operates in the same manner as a closed sensor. In addition, the station sensor may be used to change building modes.

1.3.4 PRIVILEGED VERSUS NON-PRIVILEGED CARD HOLDERS

The Alto 818 allows card holders to be defined as privileged or non-privileged. Privileged card holders have extended access and the ability to change building modes. Privileged and non-privileged cards are granted access under identical circumstances when presented to a normal or limited sensor. Table 1-3 provides a matrix for privileged versus non-privileged cards, building modes and sensor types.

Table 1-3: Privileged/Non-Privileged Access

	Building Mode	Reader Type			
		Normal	Open	Closed	Station
Privileged Card with Valid Access Code	OPEN	✓	✓	✓	✓
	LIMITED	✓	✗	✓	✓
	CLOSED	✓	✗	✓	✓
Non-Privileged Card with Valid Access Code	OPEN	✓	✓	✓	✓
	LIMITED	✓	✗	✗	✗
	CLOSED	✓	✗	✗	✗

✓ Access Granted

✗ Access denied

1.3.5 DOOR CONTROL

A number of devices may be used to control access through a door. A brief discussion of some of these follows.

Door Locks

A variety of door locks activated by electrical current can be interfaced to the Alto 818 relay outputs. Locks may be magnetic or solenoid triggered. Consideration should be given to whether a fail-safe (unlock on power loss) or fail-secure (lock on power loss) device is installed. Fail-secure locks may use mechanical override devices, such as a crashbar, for exiting if electrical power is lost. In such circumstances, doors must allow safe exit as well as entrance by emergency personnel as required.

DOOR SWITCHES

A door switch senses whether a door is open or closed. A door switch interfaces to the Alto 818 via a monitor input. Through the database setup, a door switch can serve a number of functions. It can be used to indicate a door which is held OPEN TOO LONG, exceeding the time period set with the DOOR command. Similarly, if a door switch changes state from closed to open without a valid access decision made by the ACU, a DOOR FORCED OPEN message can be generated. When anti-passback is enabled, the card holder status can be programmed to change only if the door switch indicates that the door has been opened.

REQUEST-TO-EXIT

A request-to-exit, REX, signal may be used to trigger the unlocking of a door or to inform the ACU that a door is to be opened without a valid signal from a sensor, thereby preventing a DOOR FORCED OPEN message from being generated. REX devices are frequently used on doors which use a sensor only on the entry side.

When a REX signal is used to unlock a door, the open time interval is the same as when access is granted through the sensor on the same door. The time interval may be restarted by repeatedly activating the REX input for the door. If a REX signal is generated but the door is not opened, it will relock at the end of the programmed unlock time. Just as with a door unlock triggered by a valid card key presented to a sensor, the door will relock as soon as it is opened.

REX devices can be pressure-sensitive mats, panic bars, motion detectors, push buttons or a number of other devices. The REX signal is interfaced to the Alto 818 via a monitor input.

1.3.6 ANTI-PASSBACK

If only the entrances to a controlled area are sensor-controlled, it may be possible for a key holder to pass back his or her card key to an unauthorized individual who would then be able to use it to enter the controlled area. The Alto 818 provides anti-passback control to prevent this. To use anti-passback, all entrances and exits must be controlled by sensors. Command keys must be presented alternately to an entrance and an exit; successive use of an entrance or exit constitutes an anti-passback violation. Two types of anti-passback operation are available: Hard and soft.

While an area which uses anti-passback control must have both entrance and exit sensors, exits should also be capable of being opened from the inside without use of a command key in emergency situations. National, state, and local fire and life safety codes should be checked to verify if the system design complies.

HARD ANTI-PASSBACK

When hard passback is used, failure to alternate between entry and exit causes a data log entry to be printed and access to be denied.

SOFT ANTI-PASSBACK

A soft anti-passback violation causes a data log entry to be printed but access is granted if the card key is otherwise valid.

REX AND DS CONSIDERATIONS

When an area is anti-passback controlled, a REX switch is not used at the doors. Separate doors can be used for entering and exiting or the same door may be used with readers on each side.

If an anti-passback-controlled door is not monitored by a door switch, then the ACU assumes that whenever a command key is presented to a sensor, the key holder will complete access through that door. If access of the key holder is interrupted, he or she cannot repeat key presentation without a passback violation. Use of a door switch ensures that the Alto 818 will wait until the door opens, as signaled by the door switch, before changing the key holder status. For this reason, use of a door switch is recommended in anti-passback operations.

ANTI-PASSBACK STATUS

When the Alto 818 is configured for anti-passback control at a specific door, the anti-passback status of each command key user is automatically reset from OUT to IN when the user gains entrance to a controlled area. Conversely, key holder status will be reset from IN to OUT when the key holder uses his or her command key to leave the controlled area.

Anti-passback status can be reset to UNKNOWN for all key holders by use of the FORGIVE command or for an individual key holder by use of the KEY command. If power to the ACU is lost, the status for all key holders is set to UNKNOWN.

TYPICAL ANTI-PASSBACK INSTALLATION

A typical anti-passback installation is shown in Figure 1-1. Door 1 uses a one-way mechanical turnstile which permits entrance when an authorized command key is presented to reader 1. Door 2 uses a turnstile which will permit exit when an authorized command key is presented to reader 2. Door 3 is used for two-way traffic; Reader 4 controls the entrance to the area while reader 3 controls exiting. All three entries have door switches.

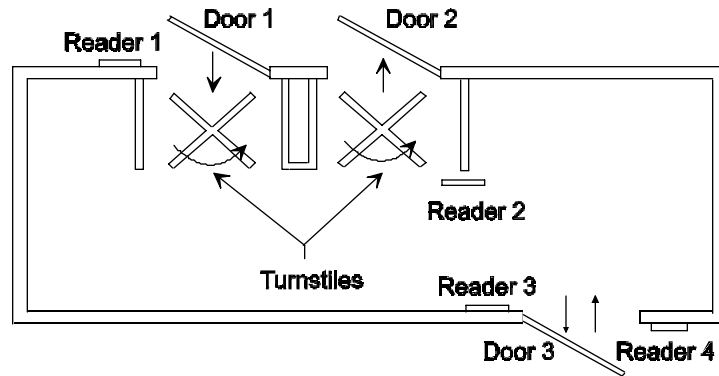


Figure 1-1: Anti-Passback Installation

1.3.7 REMOTE STATION

Remote station switches can be used to change building modes without access to the Alto 818 terminal or host. Placed adjacent to a closed sensor-controlled entry, a valid privileged card is needed to change the mode from closed to open. When exiting, the remote station switch is held down while the card is presented to a sensor. When the switch is released, the building mode changes to limited, allowing the card holder 60 seconds to exit the building before the mode changes to closed.

CAUTION:

The card holder must check that all other personnel have left the building before using the remote station switch to change the mode to closed. An alarm could be triggered by anyone remaining in the building.

1.3.8 TAMPER SWITCHES

Tamper switches detect when the enclosure of a security device has been opened. A tamper switch is built into each digital reader, keypad and the ACU. Triggering a tamper switch will cause a log message to be generated and can be defined to activate an alarm.

1.3.9 DURESS CODE

A feature of keypad use is the ability to enter a duress code. The duress code is the user's PIN with the digits shifted once to the left, e. g., 12345 is entered as 23451. Through system hardware and software configuration, the Alto 818 can display a duress event on the operator terminal, close a contact to actuate an audible alarm or initiate other actions.

SECTION 2: SYSTEM DESCRIPTION

This section describes the Alto 818 Access Control Unit (ACU) and the hardware devices available to make up a complete access control and alarm monitoring system. Current WSE hardware which may be used with Alto 818 systems is listed in Table 2-1. Older WSE products may also be compatible; contact WSE Customer Service for inquiries. A system block diagram showing an example of a system application is shown in Figure 2-1.

Table 2-1: WSE Alto 818 Compatible Products

Model	Description	Quantity per System
92818021000	SE 818SC Access Control Unit	1
92818001000	SE 818SX Access Control Unit	1
92371801000	SE 3718SU Power Supply with Battery Backup Capability	1
92301801000 ^{1, 2}	SE 3018S Power Supply	
92422230000	Alarm-Saf Power Supply/Battery Charger	1 or more for S-Net devices
92902031000 ¹	PI-1 Power Inserter - 115 VAC	
92902032000 ¹	PI-2 Power Inserter - 220 VAC	
92571010000	SE 57101 Terminal/Keyboard	1
See price list	SE 6000 Host Computer	
See price list	SE 5850 Host Computer	
See price list	NexSentry Manager	
92778001000	SE 778-A Annunciator/Control Module	1 (optional)
92774003000	SE 774-A Multiple Switch Monitor	1 to 8
92200010000 ¹	CI-1 Communications Interface	As required
92580020000 ¹	CI-8 Communications Interface	As required
92280401000 ² 92281401000 ² 92281501000 ² 92285401000 ³ 92285501000 ³	SE 2804 Analog Command Key Sensor SE 2814 Analog Command Key Sensor SE 2815 Analog Command Key Sensor SE 2854 Analog Command Key Sensor SE 2855 Analog Command Key Sensor	As required - 8 maximum
26101704001	SE 2700 Standoff for Analog Sensors	As required
92042040000 ⁴ 92042050000 ⁴ 92042051000 ⁴ 92042052000 ⁴ 92042080000 ^{1, 4} 92042260000 ^{1, 4} 92042380000 ⁴	DR 4204 DigiReader DR 4205 DigiReader DR 4205E DigiReader - Weatherized DR 4205K DigiReader with Keypad DR 4208 DigiReader DR 4226 DigiReader DR 4238 DigiReader	As required - 8 maximum
92022510000 ²	VIP2 Keypad	As required - 8 maximum
92520001000	SE 5200 Smart Modem	Optional
92043050000	NexStar RS-485 Multiplexer	As required
13100240002 13102705002 13103437002 13107721001	SE 9284 Coaxial Cable SE 9284DB Coaxial Cable SE 9284PI Coaxial Cable SE 9284E Coaxial Cable	As required
See price list	Digital and Analog Command Keys	As required

¹ These items are not UL 294 listed. They may not be used in an access control system which must meet UL 294 specifications.

² See price list for additional part numbers for different color or input voltage.

³ Supported by the SE 818SX only.

⁴ Supported by the SE 818SC only.

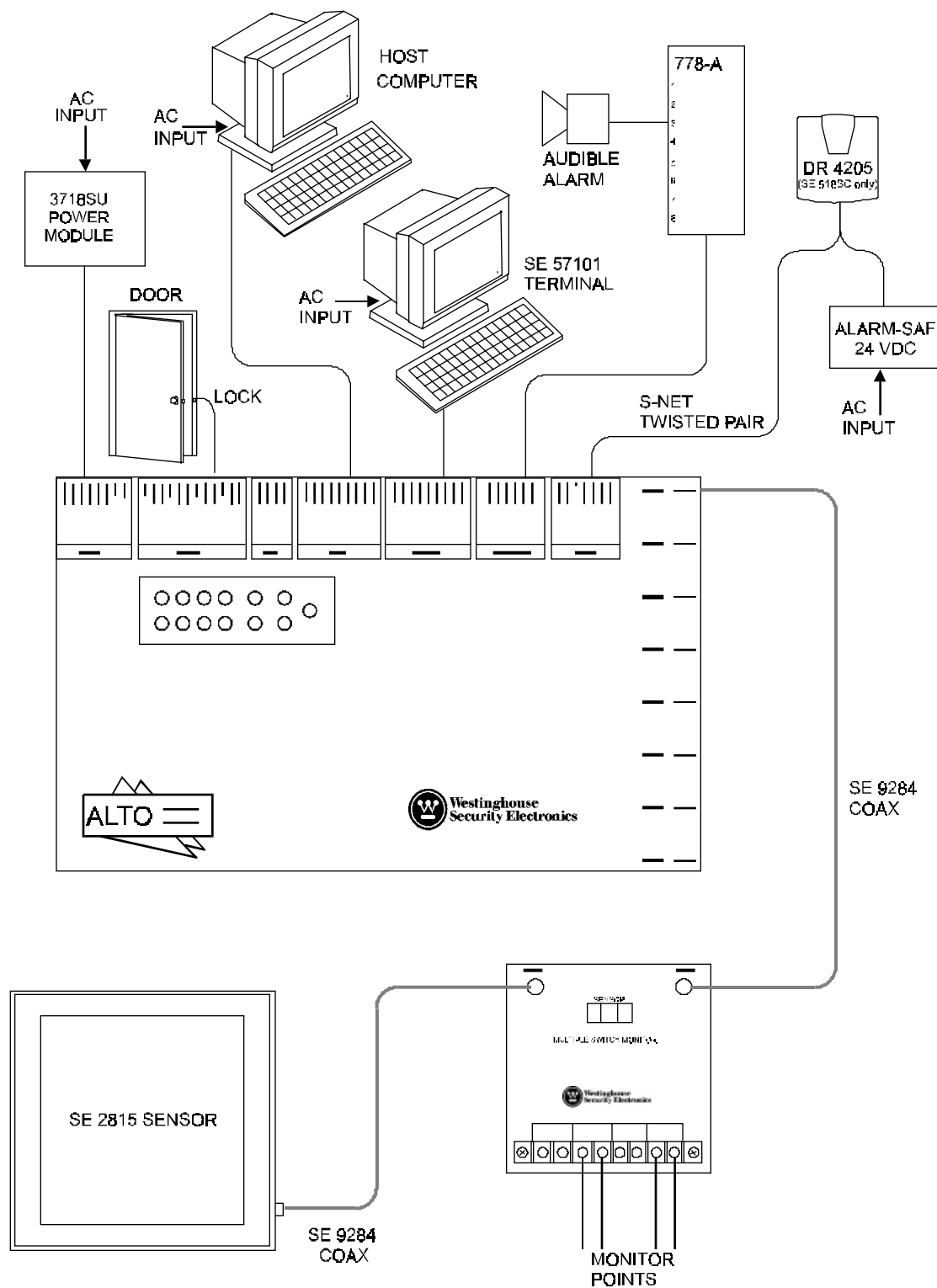


Figure 2-1: Example Alto 818 System Block Diagram

2.1 ALTO 818 ACCESS CONTROL UNIT

The Alto 818 is shown in Figure 2-2. Basic functions of the Alto 818 ACU are as follows:

- Receives identity data from readers and keypads used at controlled doors, compares this identity to a list of authorized key holders, and makes decisions to unlock doors.
- Monitors the open or closed state of controlled doors.
- Monitors the state of motion or sound detectors and window contacts and actuates control devices.
- Actuates control devices such as an audible alarm or video camera based on monitor inputs.
- Controls the building modes.
- Reports activity in the controlled area to a terminal and or host.
- Initiates modem contact with a remote host.

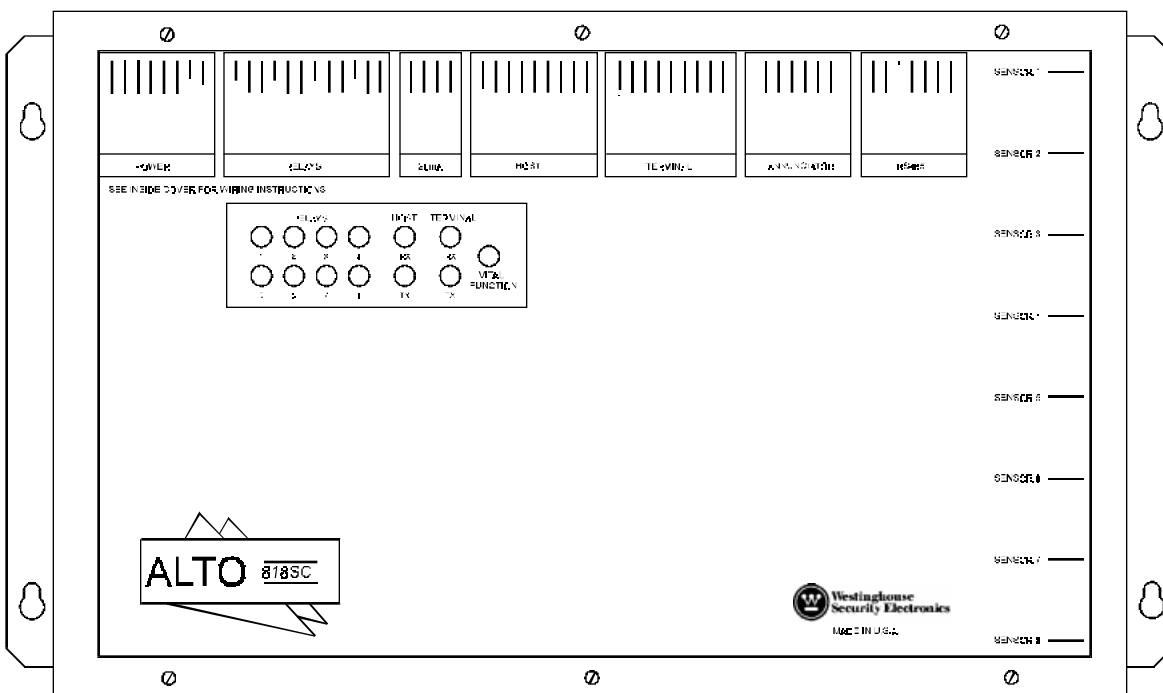


Figure 2-2: Alto 818 Access Control Unit

The Alto 818 measures 18 inches (46 cm) by 10.5 inches (27 cm) by 2.25 inches (6 cm) and weighs 5.5 pounds (2.5 kg).

2.1.1 ELECTRONICS

The major circuitry in the Alto 818 is mounted on one printed circuit assembly (PCA). Two additional PCAs, the LED panel and the auto sensing board are mounted on the system board. Other circuitry includes a DC power supply, a command key reader, door control relays, a backup battery, and reset, goof, battery and tamper switches.

LITHIUM BATTERY

A battery on the Alto 818 system PCA maintains system memory when AC power is interrupted. However, when the system is operating on the PCA battery, direct commands and anti-passback status are cancelled. The battery is a lithium 'coin cell', Rayovac or Panasonic part number BR2325. The battery will support RAM for up to 1000 hours; the battery shelf life is ten years.

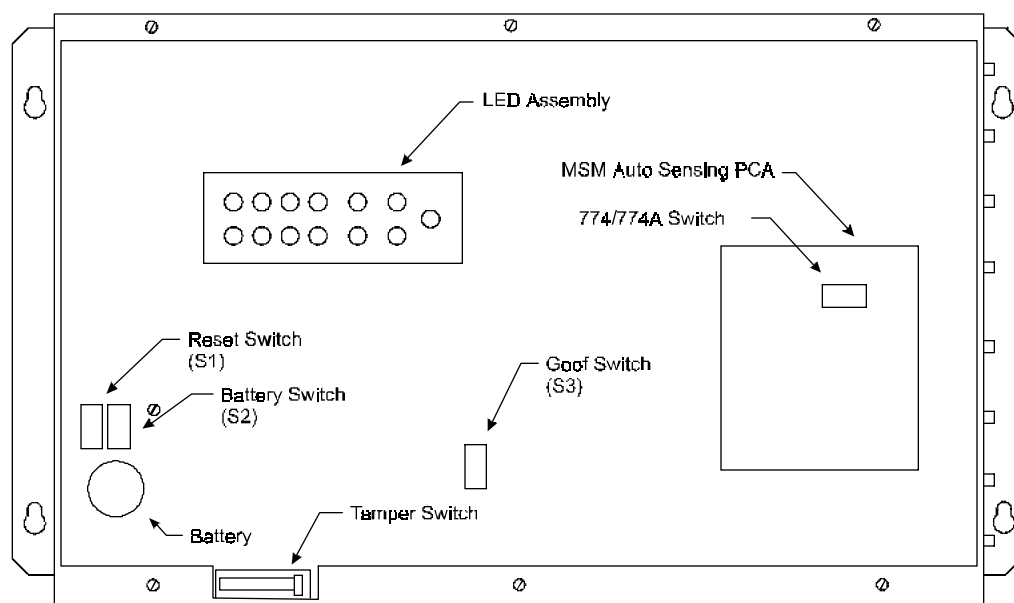


Figure 2-3: Alto 818 Battery and Switch Locations (Cover Removed)

WARNING:

LITHIUM IS A HAZARDOUS MATERIAL. OBSERVE ALL APPLICABLE REGULATIONS GOVERNING THE DISPOSAL OF SUCH HAZARDOUS MATERIAL WHEN DISCARDING THE BATTERY. REPLACE THE BATTERY WITH A 3-VOLT, BR 2325 LITHIUM BATTERY MANUFACTURED BY RAYOVAC OR PANASONIC. USE OF ANY OTHER BATTERY MAY PRESENT THE RISK OF FIRE OR EXPLOSION.

MAIN PCA SWITCHES

The Alto 818 has three switches mounted on the main printed circuit assembly: The reset switch (S1), the battery switch (S2), and the goof switch (S3). The location of these switches is shown in Figure 2-3.

Reset Switch (S1) The reset switch is a momentary-contact, push-button switch used to reset the microprocessor. In the event that the VITAL FUNCTION LED does not blink, indicating the microprocessor is not functioning properly, this switch is used to restart it. Resetting the microprocessor with this switch will not change any of the system operating parameters. It will, however, set the anti-passback status of all users to UNKNOWN and cancel operator override commands such as UNLOCK or RELOCK.

Battery Switch (S2) The battery switch is a slide switch used to connect or disconnect the lithium battery circuit. This switch is placed in the OFF position before the ACU leaves the factory, and must be placed back in the ON position when the ACU is installed. The battery switch is also used to turn off the battery circuit when changing the lithium battery or when placing the ACU in storage. When there is no power coming from a system supply, turning off the battery will cause loss of all system data.

Goof Switch (S3) The goof switch is used to gain access to the system commands in the event that the password(s) for the operator(s) with authorization rank A have become lost or forgotten, or no rank A operators are available in an emergency situation. Operating the goof switch causes the user 1 password to revert to NEW with a rank of A and the terminal baud rate to be set to the default of 300 baud.

The goof switch is operated by simultaneously pressing and holding the reset switch and the goof switch, then releasing the reset switch before releasing the goof switch.

LED PANEL

An LED panel is mounted on the main PCA and is visible through a cutout on the ACU cover. Eight LEDs, RELAY 1 through 8, illuminate when their associated door lock relays are activated. Two LEDs indicate transmit (TX) and receive (RX) activity at the terminal port, and two more indicate activity at the host port. The remaining LED (VITAL FUNCTION) flickers to indicate normal microprocessor operation.

MSM AUTO SENSING PCA

The MSM auto sensing PCA provides an interface between the system PCA and MSMs. A switch (S1) is used to configure the board to support either the earlier version of the MSM (SE 774) or the present version (SE 774-A). The MSM select switch must be to the right for use with the SE 774. In this position the 818SC will not support the 2854 sensor. The switch is set to the left for use with the SE 774-A.

2.1.2 ACU SYSTEM INTERFACE

The Alto 818 has seven connectors along the top of the unit and eight sensor connectors along the right side. System interfaces provided by these connectors are described below.

Table 2-2: Alto 818 System Interface Connectors

Connector	PCA ID	Type	Description
Power	P1	8-pin Phoenix	ACU input from power supply; power-fail and anti-tamper input.
Relays	P2	12-pin Phoenix	Eight relay outputs for door or other device control.
20 mA	P3	4-pin Phoenix	20-mA loop connection to terminal or host.
Host	P4	9-pin Phoenix	RS-232 host port.
Terminal	P5	9-pin Phoenix	RS-232 terminal port.
Annunciator	J1	DB-15	Interface to SE 778-A Annunciator/Control module.
RS-485	P6	7-pin Phoenix	S-Net port for DigiReaders and VIP2.
Sensors 1 - 8	CJ1-CJ8	F-56 coaxial	Analog proximity sensors or MSMs for doors 1 through 8.

For specific pin-to-pin interface wiring details, see Section 4.

POWER (P1)

The 8-terminal Phoenix connector labeled POWER is used to connect an AC power supply to the Alto 818. In addition to the voltage and ground terminals, one terminal (ANTI-TAMPER) can be used to connect an auxiliary anti-tamper switch. Another terminal (POWER FAIL) is used to connect a power failure signal input from the power supply. See Section 2.2 for a description of the power modules; wiring details are provided in Section 4.2.

RELAYS

The Phoenix connector labeled RELAYS provides relay contacts 1 to 8 to control up to eight door locks. If required, other devices can be controlled via these relay contacts through system configuration and the REPORT command. When used as a lock relay, the contact number must be the same as the door to which it is assigned. For interface wiring details, see Section 4.5.

The relays can support both normally open (N/O) locks and normally closed (N/C) locks. The lock type is specified through the DOOR command. A normally closed lock is defined by replying 'Y' to the REVERSE LOCK prompt. The default setting is for normally open door locks.

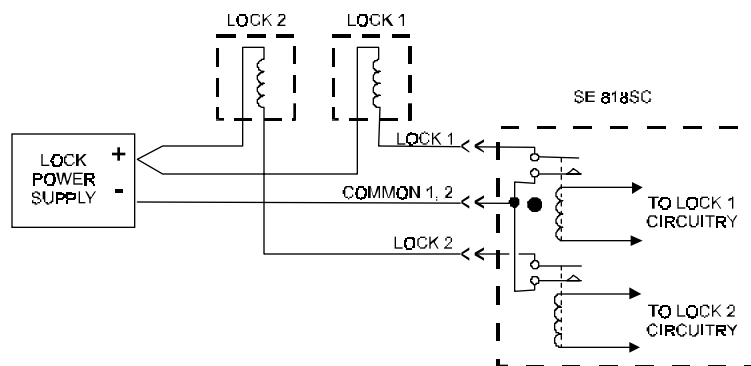


Figure 2-4: Door Lock Circuitry Block Diagram

20 mA

This connector is used to provide an interface with a terminal or host which must be located in excess of 25 feet; the terminal or host can be at a maximum distance of 2,000 feet (610 meters) from the ACU. This port and the host RS-232 port cannot be used concurrently. For 20 mA connector interface wiring details, see Section 4.10.

Host

The host connector on the Alto 818 is an RS-232C serial data port used to connect the ACU to local devices such as a host computer, a second terminal, a printer, or an external communications device. The maximum cable length from the ACU to a host port device is 25 feet (7.6 m). The data sent to the host port by the ACU is the same as the data sent to the terminal port unless specified otherwise with the REPORT command. For interface wiring details, see Section 4.7.

TERMINAL

The terminal port on the Alto 818 is an RS-232C serial data port that is used to connect the ACU to a local terminal or printer. The maximum cable length from the ACU to a terminal port device is 25 feet (7.6 m). In stand-alone mode, control of the Alto 818 is usually through this port. For terminal interface wiring details, see Section 4.7.

ANNUNCIATOR

The annunciator connector is used to connect an SE 778-A Annunciator/Control module to the Alto 818 to provide a number of monitor inputs. See Section 2.4 for a description of the SE 778-A. For interface wiring details, see Section 4.9.

RS-485

The RS-485 connector is the S-Net connector, the serial link to the DigiReader and VIP2s on the network. For interface wiring details, see Section 4.3.

SENSORS

Sensor ports 1 through 8 provide connections for analog proximity sensors or SE 774-A Multiple Switch Monitors (MSMs). Each MSM can support one proximity sensor and up to four monitor points. With a complete complement of eight MSMs, the Alto 818 can support of 8 sensors and 32 monitor points. See Section 2.5 for a description of the MSM.

2.2 POWER MODULES

A number of power modules are available for use with the Alto 818. The SE 3708CU and the SE 3718SU are UL Listed supplies which can power the ACU. The SE 3018S, SE 3018-2 and the SE 3708C are not UL Listed and may not be installed in a security system which must meet UL 294 standards. Power for S-Net devices may be supplied by the Alarm-Saf or Power Inserter power supply; the Alarm-Saf is UL Listed, the Power Inserter is not.

2.2.1 SE 3708CU / SE 3718SU POWER MODULES WITH BACKUP BATTERIES

The SE 3708CU and the SE 3718SU power modules are installed in an enclosure along with two 12-volt backup batteries (see Figures 2-5 or 2.6). These supplies can provide AC power to operate the ACU and DC power for lock control. For technical details on the SE 3708CU power module, see the *SE 3708C Uninterruptible Power Module Technical Manual*, WSE part number 66108566001. For technical details on the SE 3718SU Power Module, see the *SE 3718S Uninterruptible Power Module Technical Manual*, WSE part number 66109090001.

The SE 3708CU uses 12-volt, sealed, gel cell backup batteries connected in parallel with systems using 12-volt locks, or in series with systems using 24-volt batteries. Recommended backup batteries are listed in Table 2-3. Equivalent batteries of the same size and with a minimum capacity of 6.4 amp-hours may be used. These batteries measure 6.0 inches (152 cm) long by 3.7 inches (94 cm) high by 2.6 inches (63 cm) wide.

The SE 3718SU uses 24-volt, gel cell backup batteries. Lock voltage may be selected to either 12 or 24 volts. Recommended backup batteries are listed in Table 2-3. Equivalent batteries of the same size and with a minimum capacity of 6.4 amp-hours may be used. These batteries measure 6.0 inches (15.2 cm) by 3.7 inches (9.4 cm) by 2.6 inches (6.3 cm) wide.

Table 2-3: Recommended Power Module Backup Batteries

Manufacturer	Description	Part Number	UL File Number
Yuasa	12 V, 7.0 amp-hour, gel cell	NP7-12	MH 16464
Power Sonic	12 V, 7.0 amp-hour, gel cell	PS-1270	MH 13723
Power Sonic	12 V, 6.5 amp-hour, gel cell	PS-1265	MH 13723
Panasonic	12 V, 6.4 amp-hour, gel cell	WSE 42100189000	MH 14328

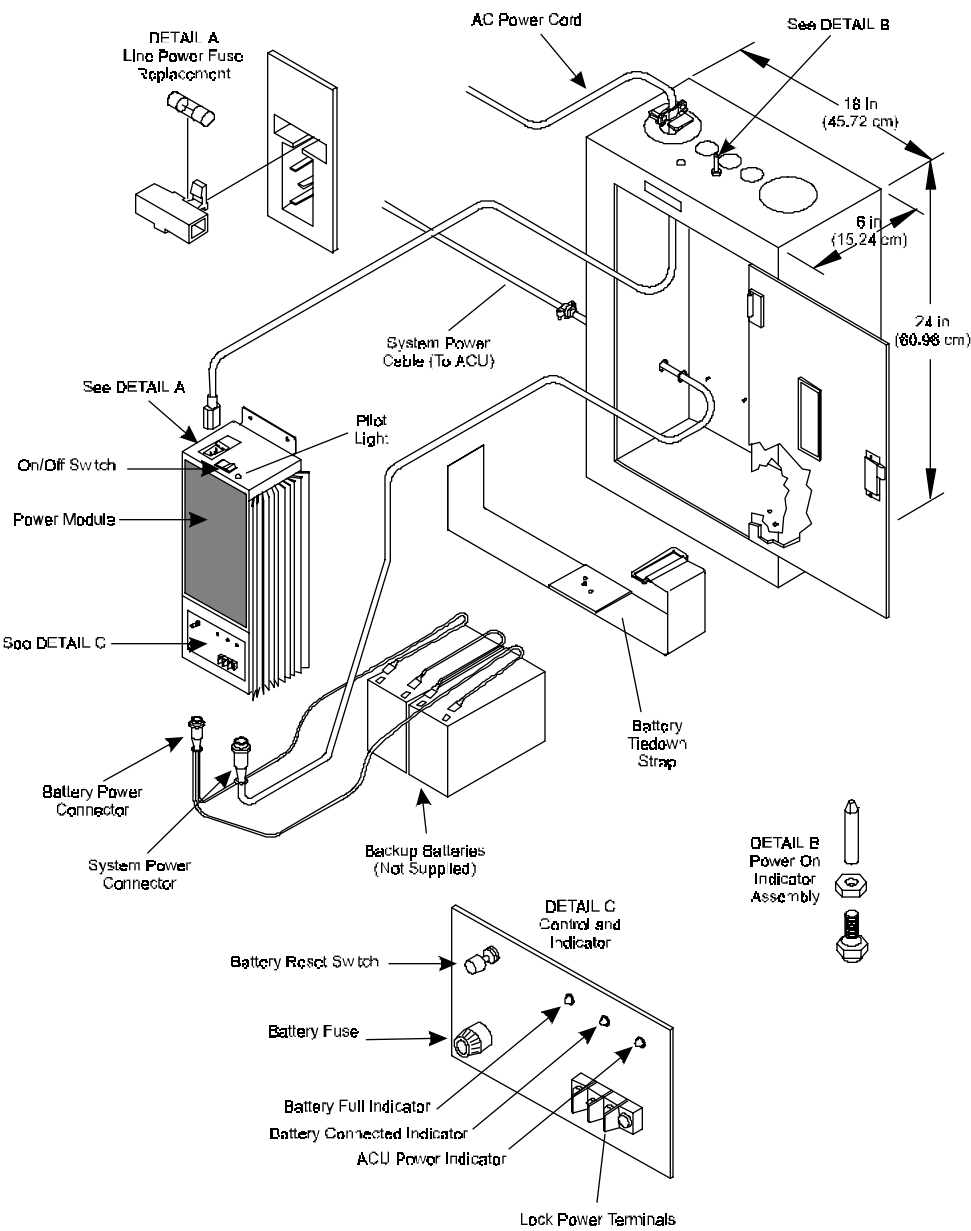


Figure 2-5: SE 3708CU Power Module with Backup Batteries and Enclosure

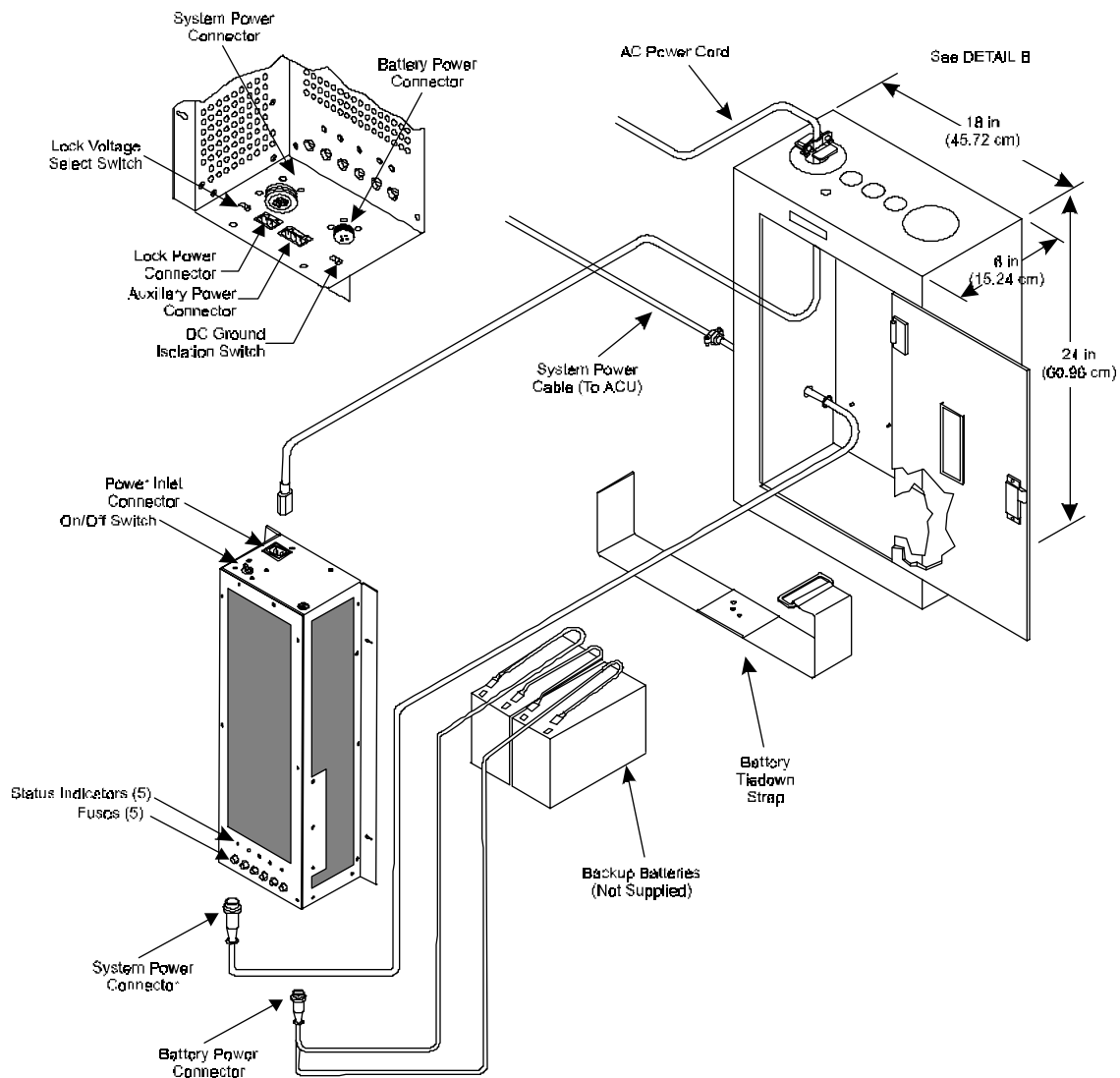


Figure 2-6: SE 3718SU Power Module with Backup Batteries and Enclosure

2.2.2 SE 3018S*/ SE 3018-2* POWER MODULES

The SE 3018S requires a 50/60HZ AC power input of 115 VAC and the SE 3018-2 requires a 50/ 60 Hz AC power input of 230 VAC. These power modules convert the line voltage to two operate an ACU; no lock power is supplied. These power modules are not suitable for UL 294 installations.

2.2.3 SE 3708C* POWER MODULE WITH BACKUP BATTERIES

The SE 3708C can operate on either a primary AC line or on a standby battery pack. At facilities without emergency power systems, the SE 3708C can provide emergency power to maintain the operation of the Alto 818 in the event of a power failure. This power module can be ordered with a 50/60 Hz AC power input of either 120 VAC or 230 VAC. In addition to the AC power for the ACU, lock power of 12 or 24 VDC is provided.

2.2.4 ALARM-SAF POWER SUPPLY/BATTERY CHARGER MODEL AS/PS5-BFS-24-UL

The Alarm-Saf Model AS/PS5-BFS-24-UL is a UL-listed 24 VDC, 4-amp power supply battery/charger which is complete with an internal stepdown transformer, and louvered cabinet with key-lockable door. The unit is thermal and reverse polarity protected. It may be used to provide DC power for S-Net devices and lock power.

Table 2-4: Alarm-Saf Specifications

Operating Temperatures	32° to 120° F (0° to 49° C)
Maximum Humidity	85% at 85° F (20° C)
Input Voltage	120 VAC $\pm$ 10%, 60 Hz, single phase
Input Current	2.5 amps, maximum
Output Power	24 VDC, regulated at 4 amps, maximum
Ripple (RMS)	0.005 VDC at 0.5 amp load, 0.350 VAC at 4.0 amps

LED INDICATORS

The Alarm-Saf Power Supply printed circuit assembly (PCA) has three LEDs to indicate operational status. These LEDs are listed and described in Table 2-5.

* These items are not UL 294 listed. They may not be used in an access control system which must meet UL 294 specifications.

Table 2-5: Alarm-Saf Power Supply LED Indicators

LED	Function
Green	Indicates that AC input power is present.
Red	Indicates that 24 VDC output is present
Yellow	Indicates a fault condition. Low battery, no AC input, blown battery fuse (Fault signal output will be generated).

FUSES

The AC input fuse and the battery charging circuit fuse are shown in Figure 2-7. Both fuses are 10-amp, AGC-10 type fuses.

BACKUP BATTERIES

Optional 12 VDC, 6.5-amp, sealed, 16 AH, lead-acid batteries (WSE Part Number 42100189001) are available and can be housed within the Alarm-Saf cabinet. Batteries above 16 AH must be housed in separate enclosures. The power supply is capable of operating with batteries of up to 38 AH.

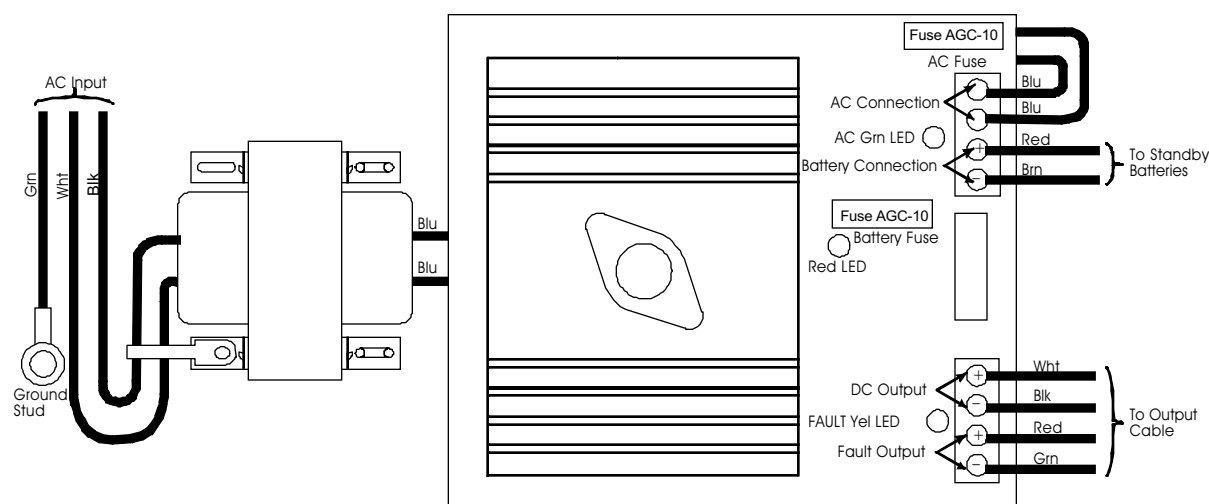


Figure 2-7: Model AS/PS5-BFS-24-UP Alarm Saf Power Supply/Battery Charger Wiring

POWER SUPPLY/BATTERY ENCLOSURE

The enclosure provides a battery space that measures 4.9 inches (11.2 cm) by 15 inches (38 cm) by 4 inches (10.2 cm). Batteries housed within the cabinet must be sealed, lead-acid batteries limited to 16 AH.

The enclosure is fabricated from 18-gauge steel, is louvered for cooling, and has a key-lockable door. The enclosure dimensions are 11 inches (28 cm) high by 15 inches (38 cm) wide by 4 inches (10 cm) deep.

2.2.5 POWER INSERTER*

The Power Inserter, PI-1 for 115 VAC or PI-2 for 220VAC, is a low-voltage, unregulated power supply and battery charger circuit. It provides output power of +24 VDC. It may be used for S-Net devices or door locks. When the AC power input fails and an optional 24 VDC backup battery is installed, the battery charger circuit activates the battery to provide uninterrupted output power. The optional backup battery is kept fully charged by the battery backup circuit and is not required for normal operation (i.e., when the AC input is present).

Connected to the Alto 818, a single PI can provide the S-Net with enough power to control up to eight doors. The specific power requirements are dependent on the types and number of devices on the net, the wire gauge used, and the total net length. Multiple PI's can be used to provide additional power.

* This item are not UL 294 listed. It may not be used in an access control system which must meet UL 294 specifications.

2.3 TERMINAL, HOST AND PRINTER

A terminal with keyboard or a host computer must be used to control the Alto 818. Both may be installed if desired. The use of a system printer is optional.

2.3.1 TERMINAL

WSE offers the SE 57101 terminal and keyboard, manufactured by Wyse, for user interface to Alto 818 systems. The terminal is connected directly to the controller through the RS-232 port.

Other terminals which emulate a Hazeltine 1500 or Qume 101 may be used in place of the SE 57101.

2.3.2 HOST COMPUTER

Three host computers are available from WSE: SE 5850, SE 6000 and NexSentry Manager. A single host computer may control multiple ACUs and provide additional capabilities. The Alto 818 connection to the host is through the RS-232 host or 20mA port on the ACU. See the appropriate host manual for details.

2.3.3 PRINTER

The SE 57184 serial interface printer is available in two models: SE 57184-S1 for 115 VAC, 60 Hz and SE 57184-S2 for 230 VAC, 50 Hz operation. The printer may be connected to the host port of the ACU, or act as a slave to a terminal or host.

2.4 SE 778-A ANNUNCIATOR/ CONTROL MODULE

The SE 778-A Annunciator/Control module, shown in Figure 2-8, connects to the Alto 818 via the annunciator connector. This module provides one latched control contact and eight non-latched contacts. Inputs are also provided for a remote station switch. The SE 778-A dimensions are 3 inches (7.6 cm) by 11.4 inches (28.9 cm) by 1.5 inches (3.8 cm).

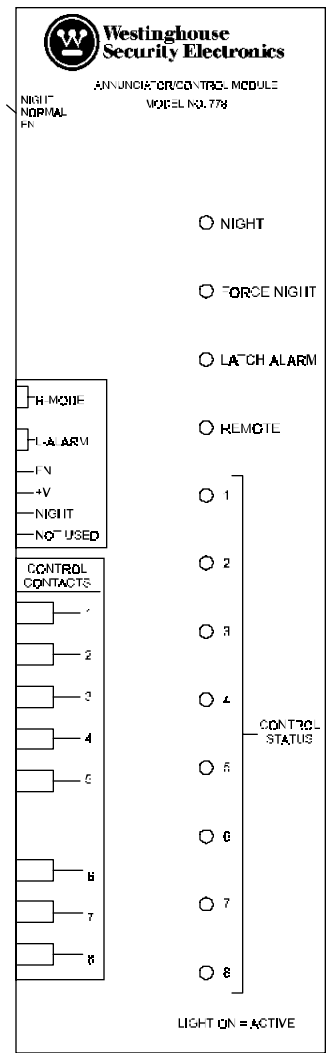


Figure 2-8: SE 778-A Annunciator/Control Module

2.4.1 LATCHED CONTACTS AND INDICATOR

The annunciator has one set of latched alarm contacts (L-ALARM) and an associated indicator light. The Alto 818 can be programmed to cause these contacts to close and to turn on the latch alarm indicator lamp when a specified abnormal condition is detected by the ACU. Once latched, these contacts will stay latched and the indicator light will stay on until the annunciator receives the SILENCE command from the Alto 818 to unlatch them. These contacts will also unlatch if the system power is recycled or if the system is reset either by use of the Alto 818 reset switch or by use of the RESET command. The latched alarm contacts are typically used to activate an audible alarm device.

2.4.2 CONTROL CONTACTS AND INDICATORS

When the Alto 818 detects an abnormal condition, it can provide a printed message at the terminal port. However, additional abnormal condition warnings or actions can be initiated through the use of the control contacts, relay outputs. The annunciator module has eight sets of normally open (N/O) control contacts with associated indicator lights that show the status of each set of contacts. Devices connected to these contacts can be activated by any of the log events defined with the REPORT command. The control contacts are rated for 120 V, 300 mA.

For most log events set up to actuate a set of these contacts, the contacts will stay closed and their indicators will stay lit until either the abnormal condition that caused them to close is resolved or the SHUNT command is used to bypass the monitor output. However, when contacts are configured to actuate on a software-controlled log events such as ACCESS GRANTED or ACCESS DENIED, the contacts close for only two seconds.

2.4.3 STATION SWITCH AND INDICATORS

The annunciator has a three-position toggle switch for changing the building mode. The three positions are: NIGHT (closed mode), NORMAL (open mode) and FN - FORCED NIGHT (limited mode). The associated LED will illuminate when a request has been made to put the Alto 818 in the limited or closed mode. This switch is activated from a remote station. In the limited mode, the indicator light on the annunciator will blink on and off. In the closed mode, the indicator light will be on continuously. In the open mode, the indicator light will be out.

2.4.4 REMOTE STATION

A remote station can be used to change building modes without requiring access to the ACU terminal or host computer. The remote station, connected to the SE 778-A module, consists of two momentary-contact push-button switches, an indicator light, associated circuitry, and a proximity reader. The reader must be identified as a station sensor with the DOOR command.

The two push-button switches (limited and closed) are used for changing building modes. To change the building mode from closed to limited, or from open to either limited or closed, the appropriate push-button is held down while a valid, privileged command key is presented to the station sensor. The building mode will change from limited or closed to open when a valid, privileged command key is presented to the station sensor without using the push-button switches. The indicator light behaves in the same manner as the light on the annunciator, described in Section 2.4.3.

2.5 SE 774-A MULTIPLE SWITCH MONITOR (MSM)

The SE 774-A MSM, Figure 2-9, provides four monitoring point contact pairs. A monitor point may be a door switch, request-to-exit switch, or other device. It is interfaced to the Alto 818 by coaxial cable connected to a sensor port. With an MSM connected to each of the eight sensor ports, the Alto 818 can monitor up to 32 points.

The SE 774-A MSM measures 6.5 inches (16.5 cm) by 5.7 inches (13.7 cm) by 2.75 inches (5.8 cm) deep.

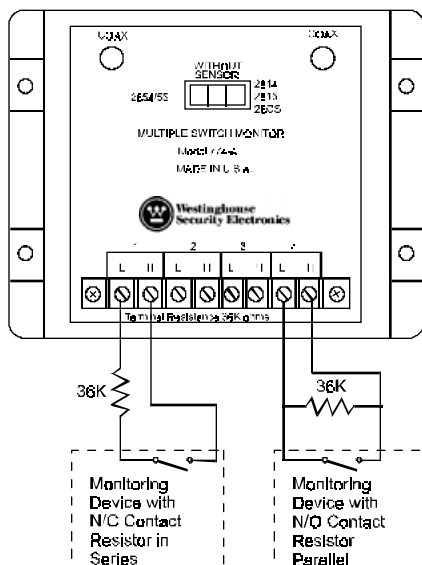


Figure 2-9: SE 774-A Multiple Switch Monitor (MSM)

NOTE:

The Alto 818 can support both the earlier version of the MSM, the SE 774, or the present version, the SE 774-A. However, all MSMs on a single ACU must be the same version. The select switch (S1) on the MSM auto sensing PCA must be set to the appropriate position for the model used (see Figure 2.3).

The monitoring points connected to the MSM must have dry electrical contacts, either normally open (N/O) or normally closed (N/C), which indicate that the monitoring device is in either the active or the inactive state.

Monitoring device connections to the MSM are by means of the terminal block mounted on the face of the MSM. The monitoring device inputs are wired by twisted pair, non-shielded cable, with a 36K-ohm resistor. The resistor is connected in series for a normally closed (N/C) contact or parallel for a normally open (N/O) contact (see Figure 2-9). A 36K-ohm resistor must also be installed across any unused contact pairs

When normally open monitoring contacts are activated, the contacts close, shorting the 36K resistor. Conversely, when normally closed monitoring contacts are activated, the contacts will open, causing an open circuit. A resistance sensing circuit in the MSM senses 36K ohms as the normal condition.

Whether the normal state is open or closed, the MSM will send a signal to the ACU indicating an abnormal condition for a monitor point. This signal consists of serial digital pulses that are decoded by the ACU during the normal polling sequence of the reader ports.

The ACU can only recognize specific monitoring contacts if they are defined with the MONITOR command during database set up. Each contact pair has a unique address in the form X.Y, where X is the sensor port to which the MSM is connected and Y is the pair number, 1 through 4.

NOTE:

If a door switch and a request-to-exit device for a given door are connected to the monitoring device contacts of the same MSM, the REX device must be connected to a contact pair with a lower number than the door switch. Otherwise, normal actuation of the REX device can cause a DOOR FORCED OPEN report to be generated and can cause an alarm device to be set off. The REX device is usually connected to contact pair 1 and the door switch to contact pair 2.

2.6 COMMUNICATION INTERFACES

WSE offers two communication interface devices which can be used to interface the Alto 818 to a host computer through the 20mA loop port. These modules can also be used to connect multiple ACUs to a single host computer. Both communications interfaces are described below.

2.6.1 CI-1 COMMUNICATIONS INTERFACE*

The CI-1 provides the circuitry to allow the Alto 818 to communicate with a host system through the 20mA loop connector. Placed within 25 feet of the host computer, the CI-1 communicates through the RS-232 port of the host. The 20mA loop output from the CI-1 can then be interfaced to multiple ACUs over a distance of up to 2000 feet (610 m).

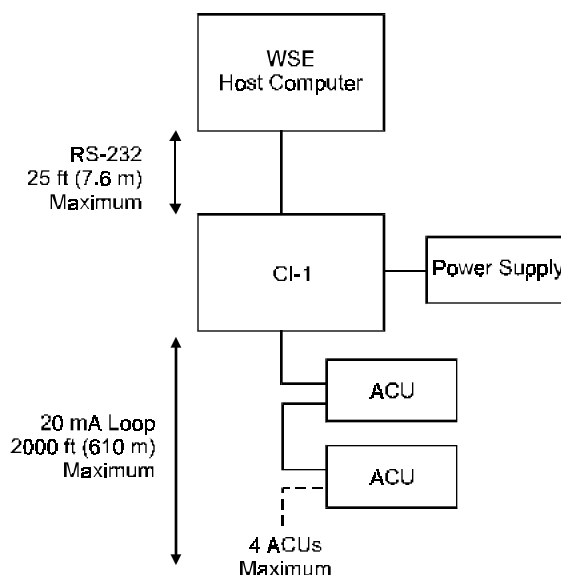


Figure 2-10: CI-1 Installation Example

* This item is not UL listed and may not be used in an access control system which must meet UL 294 specifications.

2.6.2 CI-8 COMMUNICATIONS INTERFACE*

The CI-8 is capable of driving up to eight WSE access control units through its RS-232 ports. The ACUs can be any combination Alto 818 and NexSentry systems. The each of the 20mA loop ports can support up to four ACUs. A block diagram of a security system using the CI-8 is shown in Figure 2-11.

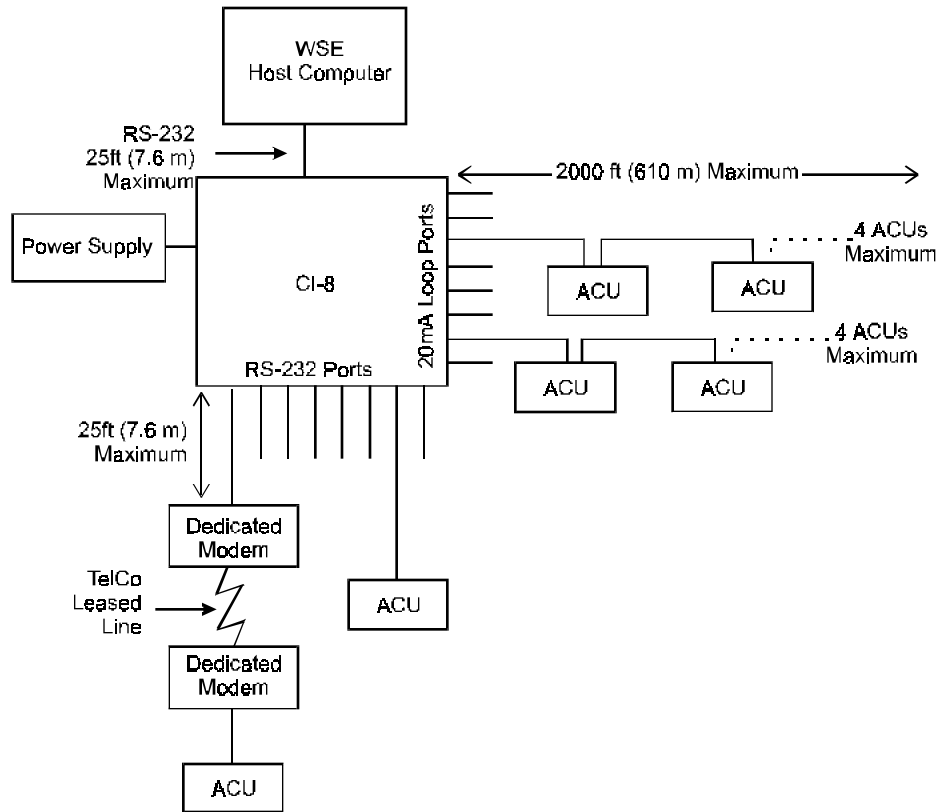


Figure 2-11: CI-8 Installation Example

* This item is not UL listed and may not be used in an access control system which must meet UL 294 specifications.

2.7 ANALOG PROXIMITY SENSORS

As indicated in Table 2-1, the Alto 818 can accommodate various analog proximity readers. These sensors are described below.

2.7.1 PROXIMITY SENSOR OPERATION

The Alto 818 ACU generates low level RF in the range of 2 to 27 MHz. This frequency range is swept from high to low and applied to the reader ports. When an analog proximity sensor is connected to one of the sensor ports via a coax cable, the sensor will emit a low power RF field from its surface which is concentrated in a region the distance of which depends upon the read range of the reader.

When a command key is placed in the region of this RF field, L/C tank circuits in the key will modulate the RF field emitted by the reader. The precise frequency of this modulated signal is a function of the tank circuits in each key. The key reader circuitry in the Alto 818 has the ability to detect this key-specific frequency and thereby to discriminate between key codes. The ACU then makes an access decision based on database parameters for each door and key code.

2.7.2 PROXIMITY SENSOR MODELS

The SE 28XX sensors consist of a loop antenna and a solid state electronics package mounted in a Lexan enclosure. They can be either surface-mounted or concealed in a wall. The reading ability of these readers is equal on both sides and is not affected by common construction materials, except metals. These sensors are 7.5 inches (19.1 cm) square, 0.67 inches (1.7 cm) deep.

SE 2814/15 PROXIMITY SENSORS

The SE 2814 sensor and the SE 2815 sensor have a read range of 2 to 4 inches (5 to 10 cm). These two sensors differ only in that the SE 2814 has the coax connector located on the rear for surface mounting using the SE 2700 standoff, and the SE 2815 has the coax connector located on the edge for recessed mounting.

SE 2854/55 MEDIUM RANGE SENSOR*

The SE 2854 sensor and the SE 2855 sensor have a read range of 2 to 12 inches (5 to 30.5 cm). These two sensors differ only in that the SE 2854 has the coax connector located on the rear for surface mounting using the SE 2700 standoff, and the SE 2855 has the coax connector located on the edge for recessed mounting.

MSM Requirements. The SE 2854/55 sensors can only be used with the SE 774-A model MSM with the MSM switch set to 2854/55.

The read range of the SE 2854/55 sensors depends upon the length of the coax to the ACU; this is the case with or without an MSM. The read range versus coax length is shown in Table 2-6.

Table 2-6: Coaxial Cable Length/Maximum Read Range

Coax Cable Length	Maximum Read Range
Up to 200 feet (0-60 m)	12 inches (30.5 cm)
200-500 feet (60-150 m)	11 inches (28 cm)
500-1000 feet (150-300 m)	9 inches (23 cm)

The SE 2854/55 medium range sensors achieve best reading performance when the command key is held parallel to the reader surface at a distance of 2 to 12 inches (5 to 30 cm).

SE 2804 COMPACT SENSOR

The SE 2804 compact sensor is intended primarily for indoor use where a small-geometry, esthetically pleasing reader is desired. The read range is 0 to 3 inches (7.6 cm) and can operate at a maximum coax length of 1,000 feet (300 M) from the ACU. The coax connector is located on the back of the unit.

A two-colored lock status LED is visible through a hole in the lower right-hand corner of the front cover of the SE 2804. Three wires, accessible through a hole in the base plate, may be used to provide optional control of this LED. The color code for these wires is shown in Table 2-7.

* The medium range sensors, SE 2854 and 2855 may be used with the SE 818SX only. They are not supported by the SE 818SC.

Table 2-7: SE 2804 Wiring

Function	Wire Color
Red LED	Red
Green LED	Green
Ground	White

The LED requires a power source in the range of +12 VDC to +24 VDC, making it able to use the same power source as door locks. When connected, the green LED will indicate an unlocked state, the red LED will indicate a locked state. +24 VDC should not be connected to both the green LED and the red LED at the same time.

2.8 DIGIREADER DIGITAL COMMAND KEY READERS*

DigiReaders emit a low-level 140-KHz field. When a digital command key is placed in this field, the key uses the field's energy to become activated. Once activated, the key responds by broadcasting a 70-KHz signal, modulated with a key-specific code sequence, back to the reader. The reader receives this signal and converts it to a digital code which is then sent to the ACU. The ACU identifies the digital command key according to its code and makes an access decision.

The digital reader series features bidirectional reading capability; digital command key cards can be read when presented to the front or back of the reader. Specifications for the DigiReaders are listed in Table 2-8 below.

Table 2-8: DigiReader Digital Command Key Readers

Model	Dimensions	Read Range**	Input Current
DR 4204	Height 7.5 in (19.4 cm) Width 1.86 in (4.72 cm) Depth 1.22 in (3.10 cm)	4 in (10.16 cm)	80 to 100 mA
DR 4205	Height 5.3 in (14.46 cm) Width 5.74 in (14.58 cm) Depth 1.27 in (3.23 cm)	6 in (15.24 cm)	50 - 80 mA
DR 4205E and DR 4205K	Height 5.3 in (14.46 cm) Width 5.74 in (14.58 cm) Depth 1.27 in (3.23 cm)	6 in (15.24 cm)	50 - 80 mA
DR 4208	Height 5.3 in (14.46 cm) Width 5.74 in (14.58 cm) Depth 1.27 in (3.23 cm)	10 in (25.40 cm)	110 to 220 mA
DR 4226	Height 17.88 in (45.42 cm) Width 9.0 in (22.86 cm) Depth 1.28 (3.25 cm)	24 in (60.96 cm)	500 mA
DR 4238	Height 26.13 in (66.37 cm) Width 13.78 in (35.0 cm) Depth 1.87 in (4.75 cm)	36 in (91.44 cm)	700 mA

DigiReader digital command key readers require a primary power source of +16 VDC to +28 VDC. A nominal 24-volt supply is recommended. For technical details on specific DigiReader models, see the appropriate WSE manual.

* The DigiReaders may be used with the SE 818SC only. They are not supported by the SE 818SX.
Maximum range given. Actual range varies with key type and installation conditions.

2.9 VIP2 KEYPAD

The VIP2 keypad may be used as a stand-alone access control device or in conjunction with a proximity sensor. The VIP2 is 4.5 in (11.4 cm) high x 4.5 in (11.4 cm) wide x 2.25 in (5.7 cm) deep. The VIP2 front panel has 12 push-button switches for PIN entry, and three LEDs to indicate door and device status.

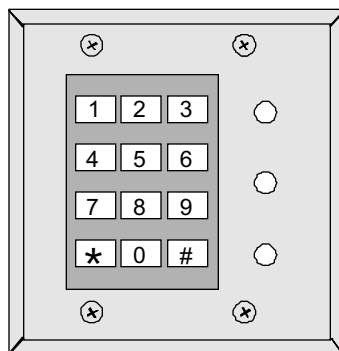


Figure 2-12: VIP2 Keypad

When the VIP2 is used as a stand-alone device, a 4- to 8-digit key code is entered for each user with the KEY command. The ACU reads this key code as if it were generated by a command key being presented to a proximity reader. However, when the VIP2 is used in conjunction with a proximity reader, a 4- to 5-digit personal identification number (PIN), generated by the ACU, is used in place of the key code.

If a user becomes aware of an error when entering code numbers, pressing either the star (*) push-button or the pound (#) push-button will abort the process and the code may be reentered. The user may have from 0 to 5 retries before an ACCESS DENIED report is generated. The number of retries is defined with the SYSTEM command as is the grace time for keypad entry. If 1 through 5 is selected, the center LED will blink on and off, indicating that the PIN entry can be retried.

2.9.1 KEYPAD USED WITH A SENSOR

When a VIP2 and a proximity sensor or a DR 4205K DigiReader with keypad is used to gain access, a valid PIN must be entered and a command card presented; the order in which this is done is not significant. Presentation of the command key to the proximity reader and the keypad entry of the PIN must be completed within a grace period as defined with the SYSTEM command. If this grace period is exceeded, the system will generate an ACCESS DENIED report after which another attempt can be made to gain access.

In this configuration, the Alto 818 generates a PIN from the command key code and the PIN seed, entered into the database with the SYSTEM command. The system-generated PINs can be displayed using the print PINS field in the PRINT KEY command.

2.9.2 VIP2 IN STAND-ALONE OPERATION

When access to a door is controlled by a VIP2 only, the PIN is the key code assigned during database setup with the KEY command. The number of keypad code digits may be 4 to 8, specified with the SYSTEM command. The option to display key codes along with ACCESS GRANTED or ACCESS DENIED reports is also provided through the SYSTEM command.

2.9.3 VIP2 LEDS

Three LEDs are visible on the VIP2. The top LED is used only when both a proximity reader and VIP2 are used at a door. In the ready state, the top two LEDs are illuminated, the bottom is not. When a valid command key is presented to the reader, the top LED goes off. Similarly, a valid PIN will turn off the middle LED. When both top and middle LEDs are off, the bottom illuminates to indicate that the door is unlocked. The LEDs return to the ready state after the door has been relocked. If the VIP2 is used without a proximity reader, the top LED will always be off.

2.9.4 DURESS CODE FEATURE

The duress code is the VIP2 code number with the digits shifted once to the left, e.g., 12345 is entered as 23451. Entering a duress code will cause a message to be displayed on the operator terminal, or the system can be configured for it to actuate contacts on the annunciator control module. Use of duress codes is enabled with the SYSTEM command.

2.10 MODEMS

Security of an Alto 818 communicating over a modem can be maintained by two methods: Building ID messages defined with the MODEM command used for identification at the remote site and requiring the remote site to call back before information is transmitted.

The Alto 818 can accommodate the following asynchronous modem types:

- Dial-up—300 - 9600 baud
- Short haul modem (line driver)
- Long haul modem

The SE 5200 smart modem is recommended for use with the Alto 818. This modem is designated as the SE 5200-L when configured as a local modem or SE 5200-R when configured as a remote modem. The SE 5200 modem runs at 9600 baud and operates on 115 VAC.

Other modems using the Hayes protocol are compatible with the Alto 818. Non-dial-up modems can be used with a leased telephone line or a direct cable between the Alto 818 and the host. The automatic dial-up function of the Alto 818 must be disabled if non-dial-up modems are used. A summarization of the similarities and differences between short- and long-haul modems is provided in Table 2-10.

Table 2-9: Short-Haul Modem versus Long-Haul Modem

Feature	Short-Haul Modem	Long-Haul Modem
Maximum distance from ACU	5 miles (8 km)	50 miles (80 km)
Uses telephone network?	No	Yes - leased line
Baud rate	Up to 9600	Up to 9600
Line conditioning required	No	No
Synchronization type	Asynchronous	Asynchronous
Transmission mode	Full duplex	Full duplex
Terminal interface	RS-232	RS-232
Line interface	5-wire	5-wire
Manual/automatic equalization	Both	Both
Desired diagnostic facilities	Remote and local loopback	Remote and local loopback

Refer to the modem manufacturer's specifications for additional requirements. Connections to public telephone line may require notification of the local telephone company.

2.11 NEXSTAR RS-485 MULTIPLEXER

The NexStar RS-485 Multiplexer provides a link between a WSE access control unit, such as the Alto 818 or NexSentry, and multiple S-Net runs. With five symmetrical ports, the end-to-end S-Net length can span up to 8000 feet (2400 meters) and contain up to 20,000 feet (6000 meters) of installed wiring.

In the simplest configuration, the NexStar allows home-run wiring which eliminates excessively long wire runs and the need to make multiple connections to a single terminal block

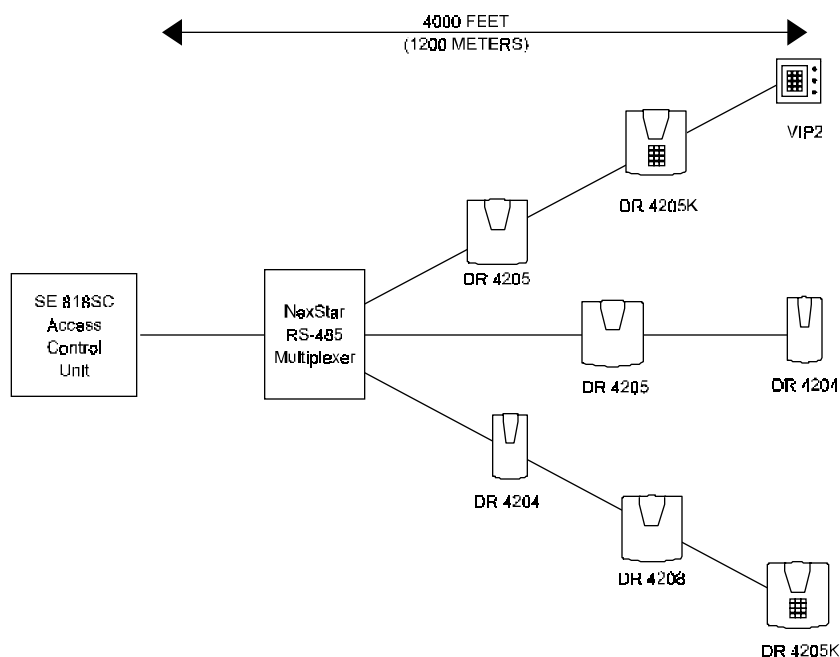


Figure 2-13: S-Net Using a NexStar

2.12 S-NET

S-Net is a serial network for communication between the ACU and digital node devices such as DigiReaders and the VIP2 keypad. Typically, the cable used is two twisted pairs with an overall shield; one pair is for data, the other pair is for DC power. Terminate the S-Net with 120-ohm, ¼ watt resistors as shown in Figure 2-14. The maximum S-Net length is 4000 feet (1200 meters).

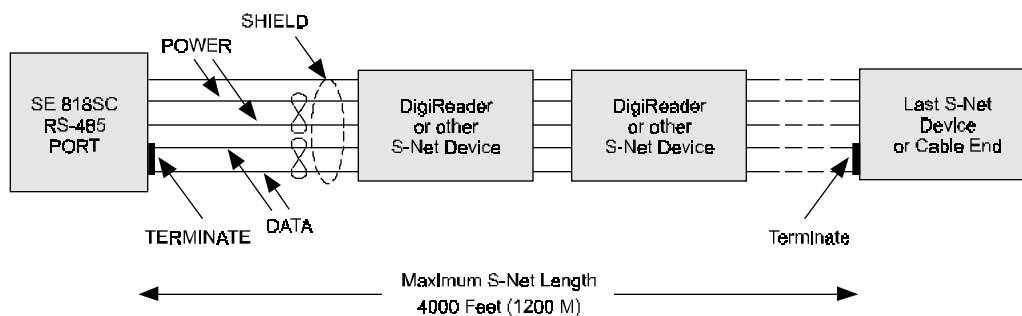


Figure 2-14: S-Net Wiring

S-Net cable should be installed as a single cable without splices or T's. If an installation requires a drop-line to a DigiReader or other device, the line should not exceed 6 feet (1.85 meters) in length.

2.13 DOOR CONTROL CONFIGURATIONS

There are many possible reader configurations. Because of their bidirectional properties, a single proximity reader may be used to both enter and exit a controlled area. Separate readers must be used on a door to allow anti-passback control. When a reader is installed on one side only, a pressure sensitive mat, panic bar, motion detector or other device can be used to send a request-to-exit signal to the ACU.

A REX switch used in conjunction with a door switch allows the ACU to distinguish a normal entry from a forced entry; if a REX signal does not precede a door switch, the ACU will report DOOR FORCED OPEN.

The Alto 818 can be configured to unlock a door when triggered by a REX signal. The door unlock time is the same as when access is granted through a reader or keypad. The time interval may be extended by repeatedly activating the REX input. I

The following sections describe configurations for a one-reader door and a two-reader door.

2.13.1 ONE-READER CONTROL

A basic door configuration with controlled entry only is shown in Figure 2-15. A DigiReader connected to the Alto 818 S-Net RS-485 port controls entry; S-Net power is provided by an Alarm-Saf supply. Two switches, a REX and door switch, are connected to the ACU through an MSM on a sensor port. A one-reader system cannot support anti-passback control.

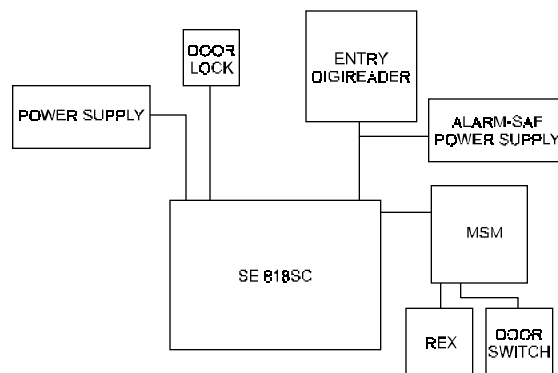


Figure 2-15: Example of One-Reader Door Control Configuration

2.13.2 TWO-READER CONTROL

The two-reader system shown in Figure 2-16 can perform functions in addition to door access. Entry is controlled by a reader on a sensor port; access can be controlled and key holder location may be recorded. The exit reader, also on a sensor port, may be used to record key holder exit, enable anti-passback control, act as a request-to-exit signal and to initiate a door unlock. In the two-reader configuration, the REX switch used for the one-door system is replaced by an exit reader. .

CAUTION:

Building exits which required valid access to unlock must be equipped with a device for emergency exit.

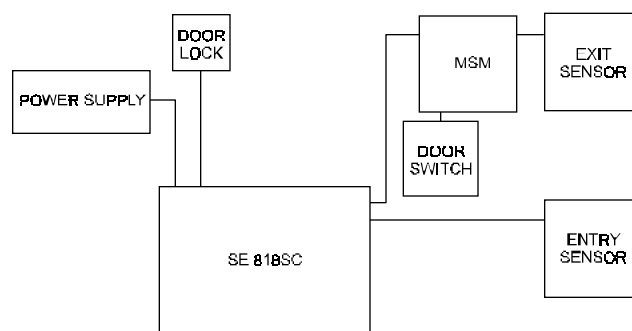


Figure 2-16: Example of Two-Reader Door Control Configuration

2.14 SYSTEM MODES

The Alto 818 system is always in one of two modes: the operate mode or the command mode. These modes are described below.

2.14.1 OPERATE MODE

The operate mode is the normal mode providing access control without the presence of an operator. No commands can be entered from the terminal while in this mode. Manual change of building modes can only be accomplished from a remote station switch. During the operate mode, all log entries are sent to the terminal and/or printer. A system operator may be assigned to monitor system activity from a terminal display.

2.14.2 COMMAND MODE

In the command mode, a user may enter commands at a terminal. To change from operate to command mode, the user must press RETURN or the space bar and enter a valid password. Commands available are determined by the user's authorization rank.

Data log entries are not printed while the system is in the command mode. Up to 4000 log entries are stored in a buffer to be displayed or printed upon returning to the operate mode. The SE 818 times-out automatically after four minutes of no keyboard activity and returns to the operate mode.

Section 6 provides a description of all commands. Section 7 describes the use of commands to create or modify the ACU database. In Section 8, use of commands for system operation are discussed.

SECTION 3:

INSTALLATION PLANNING

Section 3 discusses information required to draw up an installation plan for an Alto 818 system. Since all systems have their own particular requirements, this section can only provide general guidelines to assist in the development of an access control system.

The design of any access control system requires careful consideration of the interplay between the specific security needs of the owner and the capabilities of the available system hardware. The site security requirements should be thoroughly discussed with the owner before the system hardware is selected and an installation plan is drawn up. The owner should be made aware of what system hardware is available to implement his or her requirements. See Table 2-1 for a description of WSE hardware components compatible with the Alto 818 ACU.

The installation plan must be as comprehensive as possible and must take into consideration the exact security requirements of the owner so that the appropriate system hardware is selected and is located and set up correctly. The installation plan should be as complete as possible to avoid problems during the actual install that could result in schedule delays and budget overruns. The installation plan must be properly annotated to indicate all parameters that must be entered in the database setup sheets that are prepared prior to database setup.

3.1 INSTALLATION PLANNING

The design of any access control system requires careful consideration of the specific security needs of the owner and how the capabilities of the available system hardware can be made to meet those needs. The site security requirements should be thoroughly discussed with the owner before the system hardware is selected and an installation plan is drawn up.

3.1.1 SAFETY PRECAUTIONS

The safety precautions listed below should be taken into account when designing an installation, and they should be thoroughly reviewed before the plan is finalized. It should be noted that the Alto 818 cannot be used as the primary system for fire safety monitoring locations. However, the ACU can be used to monitor auxiliary outputs to provide supplemental information.

Safety precautions to be observed are as follows:

1. National, state, and local building and fire codes must be followed.
2. The installation plan must permit manual exit from controlled doors in the event of fire or other general emergencies.
3. The installation plan must provide for appropriate site access to emergency personnel in the event of a fire or any other emergency.
 - A. The system terminal must be accessible during an emergency so that the doors can be unlocked. Circuits that will enable monitor points to trigger the unlocking of specified emergency doors may be useful.
 - B. In the event of a power failure, emergency entrances and exits must unlock automatically. Locks on emergency doors must be rated for continuous duty. Magnetic locks, especially low current versions with inductive damping, are recommended for such applications.
4. Considerations should be made for various types of emergencies such as fires, intrusions, medical alerts, earthquakes, etc. Some codes require that emergency personnel be able to shut off all electrical power to a building from one outside location. This requirement may or may not apply to backup batteries for an uninterruptible power supply.
5. The system must be designed to avoid the accidental triggering of alarms.
6. Products which are not UL 294 listed may not be used in an access control system which must meet UL 294 specifications.

3.1.2 PLAN PROCEDURES

The development of an installation plan is an evolutionary process. First, an overall assessment is made of all access control and alarm monitoring requirements. Then the hardware items required to implement these requirements and the location of each unit is decided. At this time a preliminary installation plan can be drawn up. As requirements become more specific, this plan may change until a final plan is approved by all parties concerned.

To draw up a preliminary installation plan, the following steps must be taken:

1. Consult with the owner and determine in detail what the access control requirements are. Take notes of the meeting with the owner.
2. Obtain floor plans for all controlled areas and review them in detail with the owner. Determine the buildings and areas to be controlled making a list of all doors.
3. On the floor plan, indicate the hardware required at each location; Alto 818, system terminal, readers, switches, power supplies, monitor devices, remote stations, locks, etc.
4. Plan cable routing keeping in mind maximum run lengths. Revise placement of hardware as required. The floor plan may be helpful in estimating cable requirements.
5. Compile a list of the hardware required. Copies of Table 3-1 may be used to record WSE product requirements.
6. Review the installation plan with the owner.

Table 3-1: Installation Site Product List

Model	Description	Quantity
92818001000	SE 818SC Access Control Unit	
92371801000	SE 818SX Access Control Unit	
92371801000	SE 3718SU Power Supply with Battery BackupCapability	
92301801000 ^{1, 2}	SE 3018S Power Supply	
92422230000	Alarm-Saf Power Supply/Battery Charger	
92902031000 ^{1, 2}	PI-1 Power Inserter	
92571010000	SE 57101Terminal/Keyboard	
See price list	SE 6000 Host Computer	
See price list	SE 5850 Host Computer	
See price list	NexSentry Manager	
92778001000	SE 778-A Annunciator/Control Module	
92774003000 ²	SE 774-A Multiple Switch Monitor	
92200010000 ¹	CI-1 Communications Interface	
92580020000 ¹	CI-8 Communications Interface	
92280401000	SE 2804 Analog Command Key Sensor	
92281401000 ²	SE 2814 Analog Command Key Sensor	
92281501000 ²	SE 2815 Analog Command Key Sensor	
92285401000 ³	SE 2854 Analog Command Key Sensor	
92285501000 ³	SE 2855 Analog Command Key Sensor	
26101704001 ²	SE 2700 Standoff for Analog Sensors	
92042040000 ⁴	DR 4204 DigiReader	
92042050000 ⁴	DR 4205 DigiReader	
92042051000 ⁴	DR 4205E DigiReader - Weatherized	
92042052000 ⁴	DR 4205K - DigiReader with Keypad	
92042080000 ^{1, 4}	DR 4208 DigiReader	
92042260000 ^{1, 4}	DR 4226 DigiReader	
92042380000 ⁴	DR 4238 DigiReader	
92022510000 ²	VIP2 Keypad	
92520001000	SE 5200 Smart Modem	
92043050000	S-Net Star Coupler	
13100240002	SE 9284 Coaxial Cable	
13102705002	SE 9284DB Coaxial Cable	
13103437002	SE 9284PI Coaxial Cable	
13107721001	SE 9284E Coaxial Cable	
See price list	Digital and Analog Command Keys	

¹ Not UL-Listed; ² See price list for additional color or input voltage; ³ SE 818SX only; ⁴ SE 818SC only.

3.2 ENVIRONMENTAL REQUIREMENTS

Table 3-2 below indicates the operating range for temperature and humidity for WSE products which may be used as part of an Alto 818 access control system.

Table 3-2: Environmental Requirements for WSE Products

Device	Operating Temperature	Operating Humidity
SE 818SC/SX Access Control Unit	20°F to 120°F (-7°C to 49°C)	10 to 95% non-condensing
SE 2804 Compact Proximity Sensor	20°F to 120°F (-7°C to 49°C)	10 to 90% non-condensing
SE 2814/2815 Proximity Sensor	-50°F to 180°F (-45°C to 82°C)	10 to 100% non-condensing
SE 2804 Medium Range Proximity Sensor	-50°F to 180°F (-45°C to 82°C)	10 to 100% non-condensing
DR 4204	-4°F to 140°F (-20°C to 60°C)	10 to 90% non-condensing
DR 4205	19°F to 150°F (-7°C to 66°C)	10 to 90% non-condensing
DR 4205E and DR 4205K	-31°F to 150°F (-35 °C to 66°C)	10 to 100% condensing
DR 4208, DR 4226 and DR 4238	-31°F to 150°F (-35 °C to 66°C)	10 to 90% non-condensing
VIP2	20°F to 120°F (-7°C to 49°C)	10 to 95% non-condensing
SE 902 Power Inserter	20°F to 120°F (-7°C to 49°C)	0 to 95% non-condensing
SE 3708CU Power Supply	20°F to 120°F (-7°C to 49°C)	0 to 95% non-condensing
SE 3718SU Power Supply	20°F to 120°F (-7°C to 49°C)	0 to 95% non-condensing
SE 301S and SE 3018-2 Power Supplies	20°F to 120°F (-7°C to 49°C)	0 to 95% non-condensing

3.3 HARDWARE LOCATION

The proper location of all Alto 818 system hardware units must be determined prior to development of a final installation plan.

3.3.1 ALTO 818 CONTROLLER

The system controller should be located so that it is accessible to service personnel in the event of an emergency or a unit failure. Do not connect the lock controlling the area in which the unit itself is located unless there is an alternate method of entry.

Ensure that the proposed controller location meets all the following requirements:

- A minimum distance of 6 feet (2 meters) from main AC panels and high inductive loads (motors, pumps, etc.) unless enclosed in a metal cabinet.
- A minimum 3 feet (1 meter) from telephone cabling equipment or a public address system.
- Ambient environment free from all corrosive fumes and vapors.

3.3.2 ANALOG PROXIMITY READER

Location requirements are the same for the SE 2814/15 and the SE 2854/55* readers. These readers are suitable for both surface and concealed mounting locations. They can operate through most building materials with the exceptions of solid metal walls or expanded metal lath.

The SE 2804 compact reader is not an all-weather device and is intended for indoor surface mount only. This reader should not be mounted near metal walls or expanded metal lath.

When selecting a reader location, keep the following in mind::

- Readers should be a minimum of 6 inches (15.3 cm), as measured from the edge in the same plane as the reader, from any electrical wiring, electrical conduit, aluminum wall studs, or metal pipes.
- Readers should be a minimum of 2 inches (5.08 cm) from metal beams, walls or mesh. The SE 2700 Standoff can be used to mount readers on metal surfaces. Readers must be at least 1 inch (2.54 cm) from metal framed doors, windows or walls.

* The medium range sensors, SE 2854 and 2855 may be used with the SE 818SX only. They are not supported by the SE 818SC.

- Readers mounted in metal enclosures must have a minimum of 3 inches (7.62 cm) clearance on all sides.
- Avoid RF interference which may impair the sensor read range. Typical sources of interference include:
 - Air conditioning systems
 - Arc welders
 - Diathermy machines
 - Electric motors
 - Elevator lift motors
 - Fluorescent lighting within 2 feet (61 cm)
 - Industrial equipment
 - Radio transmitters
 - Relay panels
 - Telephone company switching panels
- Coaxial connectors and coaxial shields must not be in contact with building metal construction elements. All cable connectors should be insulated with shrink tubing or electrical tape.
- The seam between the reader and the wall or door on outdoor readers should be sealed with silicone caulking. (This requirement does not apply to brick walls where trapped humidity could damage the reader.)
- Readers must be accessible for maintenance and repair purposes.
- Reader height should be convenient for all command key holders, with consideration for those with physical limitations.

The SE 2854/55 Medium Range Readers have the following additional location requirements:

- The distance from electrical wiring, electrical conduit, aluminum wall studs, or metal pipes is increased to 12 inches (30 cm) as is the distance from metal beams.
- Readers must be located at a minimum of 12 inches (30 cm) away from metal beams.

A concealed reader must not be mounted behind rebar, wire mesh, a solid metal wall, a metal-sheathed wall, foil-backed insulating batts, or a wall painted with a lead-based paint. In the case of installations where it is absolutely necessary to locate a reader behind one of these types of walls, a 14 X 14 inches (35.5 X 35.5 cm) section of the wall must be cut away and the reader centered in this space.

3.3.3 DIGIREADER

The installer should refer to the installation manuals for the specific readers being installed. Generally, care must be taken when choosing the installation site to avoid possible external sources of RF interference. Typical sources of interference which should be considered in the location of a reader include:

- Air conditioning systems
- Arc welders
- Diathermy machines
- Electric motors
- Elevator lift motors
- Fluorescent lighting
- Industrial equipment
- Radio transmitters
- Relay panels
- PC monitors
- Telephone switching panels

Reader height should be convenient for all command key holders, with consideration for those with physical limitations.

3.3.4 REMOTE STATION SWITCH

A remote station switch, used to change building modes without access to the Alto 818 by host computer or terminal, should be located on the perimeter of the controlled area or building.

* The DigiReaders may be used with the SE 818SC only. They are not supported by the SE 818SX.

3.4 GENERAL WIRING REQUIREMENTS

The following cable and wiring requirements will satisfy normal safety standards. Refer to local standards for additional information.

- In general, no power wires should be thinner than 18 gauge.
- Ends of wires clamped under binding screws or similar parts must be tinned and terminated using a crimp tool.
- Wire splices must be insulated to withstand the same voltage and other conditions that the individual wires are required to withstand.
- Flexible power lines of any type must be protected with bushings when they pass through walls and sheet metal.
- All S-Net devices are connected with twisted pair wire plus shield.

Grounding of the Alto 818 system, its power supplies, and all node devices is essential to guarantee proper system operation. The system must be "single-point grounded." All signal grounds and all chassis grounds are connected to the ground terminal of the ACU power supply. This, in turn, is connected to earth ground via the AC circuit. Unplugging the power supply from the AC wall outlet should "float" the entire system; with the power supply unplugged there should be no continuity between earth or building metal ground and any conductive part on the ACU or any of its system devices.

In general, the S-Net shield should be grounded at one end only. If noise problems or other symptoms such as incorrect reads or false error messages occur when the system is first powered on after installation, contact WSE Customer Service for assistance.

3.5 COAXIAL CABLE INSTALLATION

The correct installation of coax cable will minimize the time and cost of the system installation. When not installed in accordance with the rules provided below, system faults may occur that are difficult to isolate.

- Coaxial cables used on Alto 818 installations must be SE 9284-type cables. Substitutions are not permitted unless written approval is obtained from WSE. See Appendix C for a list of approved cable vendors.
- Maximum run length of coax cables must be held to 1,000 feet (305 meters).
- Do not ground coax cable shield - this will cause ground loops.
- Reader coax cables and lock cables may share a common conduit run. However, bundling or sharing conduit runs with other building cables should be avoided. Use care in parallel runs keeping coax at least 6 feet (1.8 m) from high voltage (>24 VAC) lines or 3 feet (1 m) away when in grounded conduit.

Never bundle or run coax cables with high energy cable. Low energy signal wires (coax cable or shielded wire types) that carry signals outside the 1.5 to 27.5 MHz range may be bundled with the sensor cables. Paging system wiring is prohibited.

- Avoid splicing coax cables. If splicing is necessary, terminate both ends with a crimped connector and then use an F-81C barrel connector. Shrink tubing or electrician's tape must be used to protect against ground faults on all splices. No solder splices are allowed. Silicone grease on the threads is advised in extremely damp locations.
- Plastic cable clamps and tie-wraps must be used to secure cables to beams, walls, and ceilings. Staples must never be used. Clamps must not be tightened so that they distort the cables. Running cable in wire troughs, cable hooks, and conduit is preferred; loose bundling is required. Use care when pulling coax.
- Coax cable should not be mechanically distorted. Cable bends must have a minimum radius of one inch (2.54 cm). Service lengths of cable must not be coiled.
- Coax cables should not be exposed to rain or underground water. When cables will be buried or otherwise come in contact with water, all-weather WSE approved types such as SE 9284DB SE 9284PL, or SE 9284EL must be used.
- Use F-56 type cable connectors only. Use a the proper size crimp tool, do not leave the crimp ring loose and do not over crimp. Avoid cutting the center conductor too short T-splitters are not permitted.

3.6 S-Net

S-Net is an RS-485 serial network for communication between the ACU and node devices. Typically, the cable used is two twisted-pairs with an overall shield; one pair is for data, the other pair is for DC power. It is recommended that separate data and power cables be used when the length exceeds 500 feet (150 meters). Table 3-3 lists recommended cable.

Table 3-3: S-Net Cable Recommendations

	Type	Description	Gauge
S-Net Length < 500 Feet Data and Power	Belden 9552	2-Pair	18 AWG
	Belden 1069		16 AWG
S-Net Length > 500 Feet Data Only	Belden 9841	1-Pair	24 AWG
S-Net Length > 500 Feet Power Only	Belden 9341	2-Conductor	18 AWG
	Belden 9342		16 AWG
	Belden 9343		14 AWG

3.6.1 CABLE LOSSES

Power loss over distance will effect the performance of network devices. The length of the S-Net can be up to 4000'. To power a 200mA reader at this distance requires a wire gauge of 16 AWG or larger. For a single run, this allows 16VDC at the node if 24 VDC is the source.

Table 3-4: S-Net Typical Wire Loss (18 AWG)

Device	Minimum Voltage Required	Power Required	S-Net IR Drop/1000 Ft
DR 4204	16 VDC	1.96 Watts	0.84 Volts
DR 4205	16 VDC	1.96 Watts	0.84 Volts
DR 4208	16 VDC	4.8 Watts	2.4 Volts
DR 4226	16 VDC	9.6 Watts	4.8 Volts
DR 4238	16 VDC	12 Watts	6 Volts
VIP2	16 VDC	0.98 Watts	0.42 Volts

3.6.2 S-NET POWER WIRE SIZE

The daisy chaining of S-Net devices causes significant cable losses. At least 16 volts must be available at each node to insure proper operation. The following steps will help determine the proper wire gauge for an installation.

1. Find the total number of load units from the Device Load Table below. Add only the devices on the S-Net that are at least 50 feet (15 meters) from the power supply.

Table 3-5: S-Net Device Load

Device	Load Units
DR 4204	2 Each
DR 4205	2 Each
DR 4208	4 Each
DR 4226	8 Each
DR 4238	10 Each
VIP2	1 Each
Magstripe (MSR)	1 Each

2. Using the Power Wire Size table below, the cable gauge is the intersection of the row containing the accumulated number of loads and the column with the S-Net length.

Table 3-6: Power Wire Size

Load Units	Distance						
	500 Ft	750 Ft	1000 Ft	1500 Ft	2000 Ft	3000 Ft	4000 Ft
5	24 AWG	22 AWG	22 AWG	20 AWG	18 AWG	16 AWG	16 AWG
10	22 AWG	20 AWG	18 AWG	16 AWG	16 AWG	14 AWG	12AWG
15	20 AWG	18 AWG	16 AWG	16 AWG	14 AWG	12 AWG	10 AWG
20	18 AWG	16 AWG	16 AWG	14 AWG	12 AWG	10 AWG	8 AWG
25	18 AWG	16 AWG	14 AWG	12 AWG	12 AWG	10 AWG	8 AWG
30	16 AWG	14 AWG	14 AWG	12 AWG	10 AWG	8 AWG	
35	16 AWG	14 AWG	14 AWG	12 AWG	10 AWG	8 AWG	
40	16 AWG	14 AWG	12 AWG	8 AWG	8 AWG		

An example system might contain the following S-Net devices: 1 Alto 818 ACU, 4 DR 4205 DigiReaders, and 4 VIPs. The loads are loads are: $4 \times 2 = 8$ for the DR 4205s and $4 \times 1 = 4$

for the VIPs for a total of 12. The distance to the last device is 1200 feet. Looking at the row for 15 loads and the column for 1500 feet; the required wire size for this S-Net power pair is 16 AWG.

3.6.3 ALTERNATIVES TO LARGE POWER WIRE

If the wire size from the table is very large, there are alternatives:

1. A second power supply can be located closer to the devices to limit the total length.
2. Two or more conductor pairs can be used to increase the load capacity.

2-26 AWG $\approx$ 1-22 AWG

2-20 AWG $\approx$ 1-18 AWG

2-18 AWG $\approx$ 1-16 AWG

If the size gets too large to “fit” into the compression terminal blocks then a splice can be made from 16 awg to the required larger wire.

NOTE:

The communication pair does not need to duplicate the power pair size. The data pair should remain a twisted shielded pair of 22 or 24 awg.

3.6.4 FUTURE SYSTEM EXPANSION

Keep in mind that the wire size chosen for the installation must accommodate future system growth. If more doors are to be monitored in the future, consider the alternatives:

- Use larger wire to accommodate the additions, or
- Plan to add a power supply for the new doors.

3.6.5 S-NET CABLE

The S-Net cable is generally described as “two twisted pairs with an overall shield” (one pair for power and one pair for communication). When separate power and communications cables are used, attach the shields together.

S-Net cable should be installed as a single cable; splices should be soldered or secured with crimp lugs. Drop-lines to a S-Net devices should not exceed 6 feet (1.8 meters) in length.

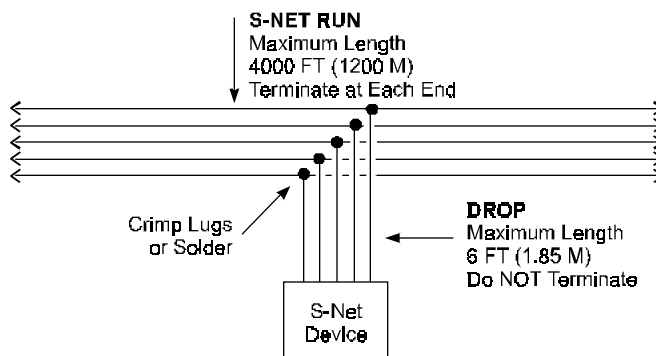


Figure 3-1: Drop Wiring

3.6.6 TERMINATION RESISTORS

The S-Net should be terminated with a 120-ohm, ¼ watt resistor connected between the wires (DATA A and DATA B) at the last node device on each branch of the S-Net.

3.6.7 NEXSTAR RS-485 MULTIPLEXER

The NexStar multiplexer may be used to create multiple S-Net branches and increase overall network length. All S-Net runs must be terminated at each end with a 120-ohm, ¼ watt resistor between the data lines. Figure 3-2 shows a sample block diagram indicating where termination resistors must be installed. See the NexStar manual for further information.

Figure 3-2: S-Net Termination

3.6.8 WIRE INSERTION

For wire insertion to either fixed block or Phoenix connectors, the following procedure is recommended:

1. Strip the wire end.
2. Twist the exposed strands tightly and tin the ends.
3. Crimp an appropriate size ferrule on the end of the wire. Be sure that the ferrule is crimped on bare conductor metal, not the insulation.

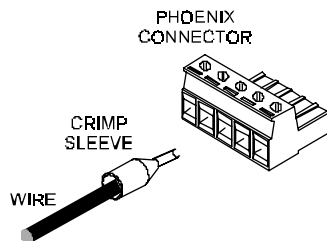


Figure 3-3: Wire Insertion

4. Insert ferrule in the appropriate Phoenix connector terminal. Tighten the connector binding screw and torque to 5 inch-pounds (0.56Nm).

3.7 S-NET POWER REQUIREMENTS

One or more power supplies are required to provide DC power to the S-Net devices. The specific number of power supplies will depend on the number of devices and the overall length of the S-Net cable. Table 3-7 provides a list of nominal power as a guideline to determine power needed.

Table 3-7: S-Net Device Supply Requirements

Device	Minimum Voltage Required	Power Required	S-Net IR Drop/1000 Ft
DR 4204	16 VDC	1.96 Watts	0.84 Volts
DR 4205	16 VDC	1.96 Watts	0.84 Volts
DR 4208	16 VDC	4.8 Watts	2.4 Volts
DR 4226	16 VDC	9.6 Watts	4.8 Volts
DR 4238	16 VDC	12 Watts	6 Volts
VIP2	16 VDC	0.98 Watts	0.42 Volts

Power supplies may be placed in-line at the controller PCA or at intervals along the S-Net cable. See the power supply manual for installation details.

3.8 ALTO 818 MOUNTING

The Alto 818 should be installed in an electrical equipment cabinet such as a NEMA Type I Panel Enclosure or any other enclosure that is designed to house electrical and electronic controls that do not require an oil- or dust-tight atmosphere. All devices should be mounted on nonconductive surfaces, so devices are not grounded to the building when AC power is removed.

The SE 3708CU or the SE 3718SU power modules can be located in the same cabinet as the Alto 818. Neither the SE 3708CU nor the SE 3718SU should be mounted below the ACU as the heat generated by the power module can raise the ambient temperature of the ACU beyond its maximum acceptable limit. Mount the SE 3708C or the SE 3718S vertically so that it receives proper airflow around the heat sink.

If the temperature inside the enclosure is found to rise to 120° F (49° C) or more, cut ventilation holes or slots in both the bottom and the top of the enclosure. If natural convection air current is insufficient to prevent an ambient temperature of less than 120° F, a cooling fan must be used to force cooling air through the enclosure.

To mount the Alto 818, observe the following restrictions:

- Wiring clearance is 6 inches (15 cm) around the edges of each unit.
- Service clearance is approximately 8 inches (20 cm) at the front of each unit.
- Adequate enclosure ventilation must be provided. Install a cooling fan if required.
- Anti-tamper switch is installed on enclosure door.

3.9 CONTROLLED DOORS

Early in the development of an installation plan, a list of controlled doors should be prepared. For each door, the list should specify whether one or both sides of the door will be controlled. Specify which doors are emergency doors which should be configured to unlock in the event of an emergency. List the lock type, reader, sensors, keypads and switches to be used.

3.9.1 UNMONITORED DOORS

Although they may have either an outside reader or both an outside and an inside reader, access controlled doors are said to be unmonitored if they do not have a door switch connected to the Alto 818. The ACU will not detect when such doors are forced open or left open too long. These doors will relock only when the unlock time runs out. A monitored door may be changed to unmonitored by shunting the door switch with the SHUNT command.

3.9.2 DOOR LOCKS

WSE recommends that all controlled devices, including door locks, be rated for continuous industrial duty. All auto-unlock and reverse action locks must be rated for continuous duty. All locks must be capable of operating within the full range of the lock power supply.

3.10 MULTIPLE SWITCH MONITORS

To determine the number of MSMs that will be required to interface the Alto 818 with the system hardware, mark the installation plan to indicate all points to be monitored. Four monitor contacts may be connected to each MSM. Each MSM can support one analog proximity reader by means of a coax cable. Indicate the door lock connections which are routed to the lock outputs of the Alto 818 on the installation plan.

3.11 MONITORED INPUTS

Monitored inputs are any contacts connected to the ACU through an MSM. Each monitored contact has a designator in the form X.Y, where X is the sensor port of the MSM (1–8) and Y is the contact pair number (1–4). Monitor points used for door switches and REX switches are selected with the DOOR command. The MONITOR command may be used to enter a name for each point and to indicate a report number to be initiated when the monitor point is active.

When both a REX and door switch are to be used on a door, the REX switch must have a lower designator number than the door switch. For an MSM connected to sensor port 2, the REX switch might be contact pair 1, monitor point 2.1, and the door switch contact pair three, monitor point 2.3.

3.12 INSTALLATION SEQUENCE

The following is a suggested order for installing a Alto 818 security access system. If the installation is an upgrade or an addition to an existing system, the procedures will vary.

CAUTION:

Do not power up the system until the wiring is complete and has been double-checked.

1. Complete the installation plan.
2. Install S-Net, monitor input and relay output wiring. Install coaxial cable for analog sensors and MSMs.
3. Mount the Alto 818, SE 778(s), SE 774(s), one or more power supplies and make the wire connections between them. **DO NOT POWER UP!**
4. Mount readers and door hardware.
5. Terminate wiring to readers and hardware.
6. Terminate wiring to the Alto 818.
7. Power-up and perform initial testing.

SECTION 4: WIRING

This section provides the product information necessary to install an Alto 818 access control system. Because each installation site is unique, only general guidelines for an installation plan can be given. Specific power and environmental requirements are listed for each WSE product which may be included in the security system. Connectors, pin-outs and wiring connections are given.

All installation wiring shall be in accordance with the National Electrical Code ANSI/NFPA70.

Installation according to this manual will meet specifications for a UL 294 access control system. A UL 294 access control system must be tested annually as described in Section 9.

4.1 AC POWER

The SE 3708CU or the SE 3718SU power module is connected to both the primary AC line power and to the ACU. If required, the SE 3708CU or the SE 3718SU can be connected to backup battery power.

Both the SE 3708CU and the SE 3718SU power modules require a 115 VAC ($\pm 10\%$), three-wire (single-phase) primary power circuit with a low resistance ground (green) conductor. This input power line must have a dedicated circuit breaker providing AC power to the power module and any modems in the system. WSE recommends that a constant voltage transformer with a spike filter be placed in this line.

The primary power cable may be either exposed cable or in conduit. Its gauge and wire type must meet the requirements of the National Electrical Code and it must have low resistance through its earth-ground connection.

Use of an AC line with more than one AC circuit can result in electrical noise from other devices such as motors, etc. Use of a non-dedicated AC circuit can cause unacceptable variations in power to the power modules. The ideal power source is a dedicated uninterruptible power supply for the Alto 818 system.

When the Alto 818 and a terminal/printer are connected via null modem cables, they must use the same AC line and/or the ground points must be at the same physical connection point.

4.1.1 GROUNDING

The building codes in many cities allow two-wire AC with conduit for ground. WSE recommends that the electrical contractor should be directed to run two conductors with a separate ground wire.

4.1.2 ACU CONNECTION

The SE 3708CU and SE 3718SU power modules are connected to the ACU by a 6' 5" shielded, 9-conductor cable supplied with the power modules. The cable plugs into the power connector on the Alto 818. Refer to Figure 4-1 for wiring diagrams of these connections.

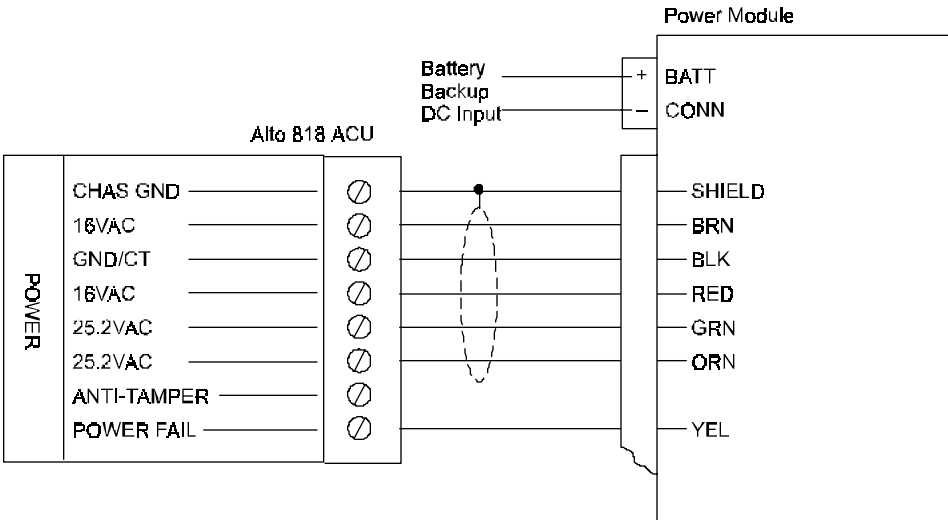


Figure 4-1: SE 3708CU or SE 3718SU Power Module

The SE 3708CU provides a 40VAC, peak-to-peak, 400Hz square wave power input and a 80VAC, peak-to-peak, 400Hz square wave power input to the power connector. In addition, the SE 3708CU connects a power failure signal (YEL conductor) to the Alto 818 power failure terminal.

4.2 DC POWER

A DC power source is required for S-Net devices. One or more supplies may be required depending on the type and number of devices used in the system. A discussion of power requirements for WSE products and how to estimate system power needs can be found in Section 3.

4.2.1 ALARM-SAF MODEL AS/PS5-BFS-24-UL

The optional 12VDC, 6.5-amp, sealed 16 AH, lead-acid batteries (WSE part number 42100189001) are available and can be housed within the Alarm-Saf cabinet. The Alarm-Saf power supply is capable of operating with batteries up to 38 AH but batteries above 16 AH must be housed in a separate enclosure.

The Alarm-Saf has two fuses, one for AC input, the other for the battery charging circuit. Both fuses are 10-amp, type AGC-10.

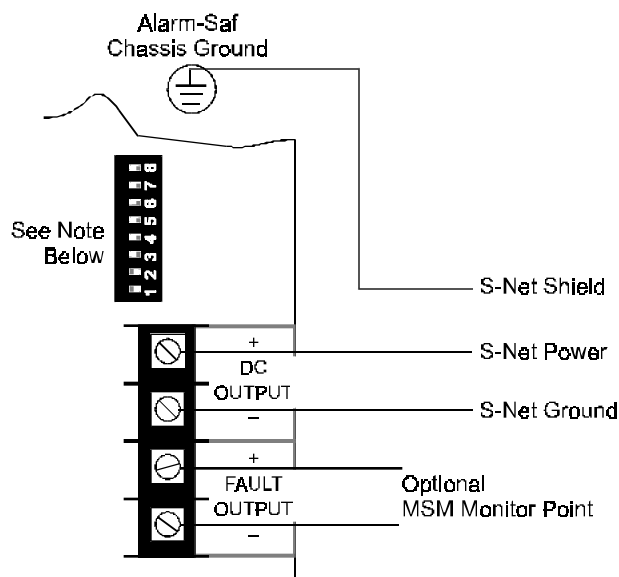


Figure 4-2: Single Alarm-Saf Power Supply Installation

SINGLE ALARM-SAF INSTALLATION

Installation of a single, or the first of multiple, power supplies is shown in Figure 4-2. The Alarm-Saf supply Fault Output signal may be monitored through a contact pair on an MSM.

NOTE:

The Alarm-Saf will have either an 8-position DIP switch or an 8-line block mounted in the position shown. Switches 3 through 8 should be set to the right; switches 1 and 2 should be set to the left. Lines 3 through 8 should be severed; lines 1 and 2 should remain intact.

MULTIPLE ALARM-SAF POWER SUPPLIES INSTALLATION

When more than one Alarm-Saf power supply is required, the installation for additional supplies should be as shown in Figure 4-3. The Fault Output signal of each additional supply may be monitored through a contact pair on an MSM.

WARNING:

FAILURE TO FOLLOW THE INSTRUCTIONS BELOW MAY RESULT IN EXTREME DANGER OF AN ELECTRICAL FIRE.

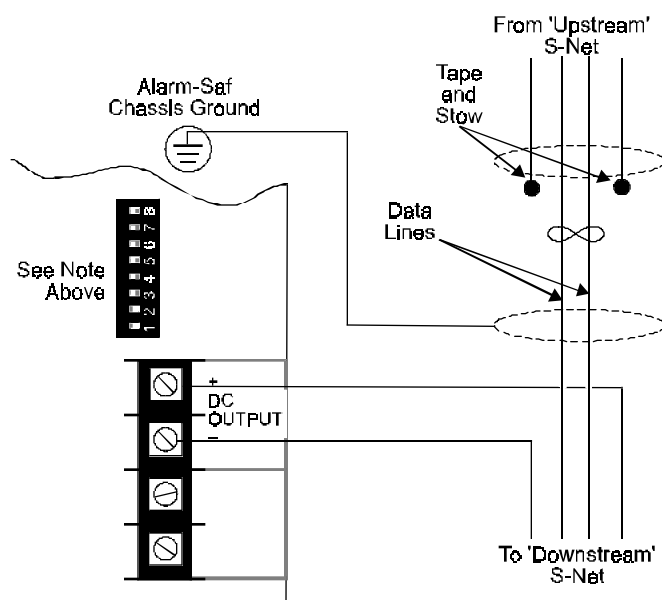


Figure 4-3: Multiple Alarm-Saf Power Supplies Installation

1. Verify that all installed power supplies to the S-Net are OFF.
2. Carefully cut through the S-Net cable shield.
3. Cut the power lines.
4. Tape and stow the power lines from the upstream S-Net.
5. Connect the downstream power lines to the supply.
6. Connect the downstream shield to chassis ground of the power supply.
7. Connect the fault output to monitor points as required.

4.2.2 POWER INSERTER

The Power Inserter, PI-1 or PI-2, can be equipped with battery backup. Separate connectors provide power for S-Net devices and door locks. When multiple PIs are used, connectors J1 and J2 can be used to chain power supplies along the S-Net.

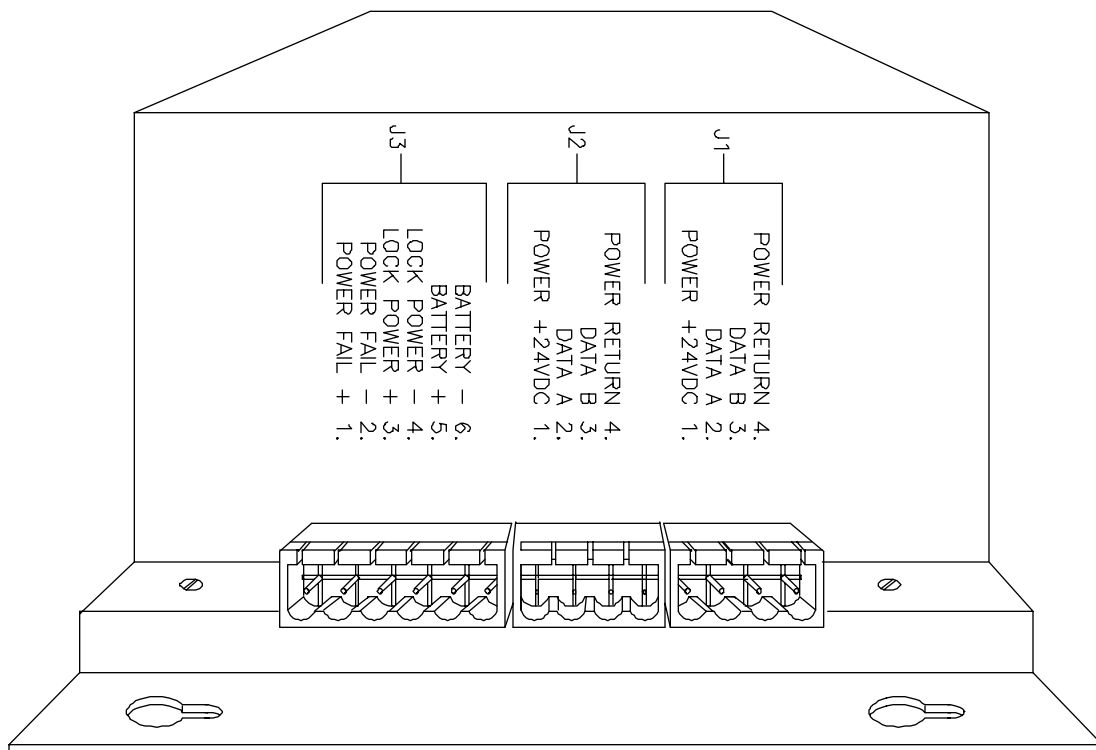


Figure 4-4: Power Inserter End View

Table 4-1: Power Inserter Pin-Outs

Connector	Description	Pin	Description
J1	S-Net	1	+24 VDC
		2	Data A
		3	Data B
		4	24 V Return
J2	S-Net	1	+24 VDC
		2	Data A
		3	Data B
		4	24 V Return
J3	Power	1	Power Fail +
		2	Power Fail –
		3	Lock Power +
		4	Lock Power –
		5	Battery +
		6	Battery –

SINGLE POWER INSERTER INSTALLATION

Figure 4-5 shows the installation of a single PI providing S-Net power.

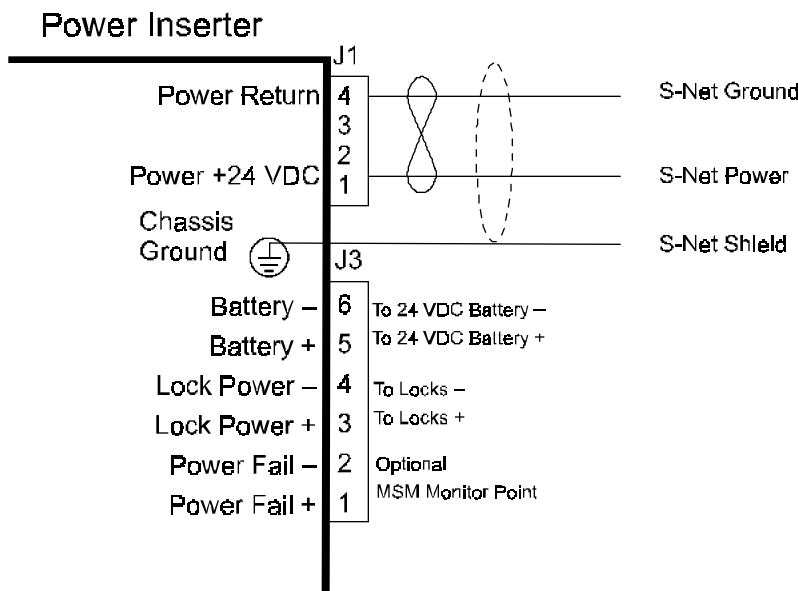


Figure 4-5: Single Power Inserter to S-Net Wiring

MULTIPLE POWER INSERTERS INSTALLATION

Installation of additional Power Inserters is shown in Figure 4-6.

WARNING:

FAILURE TO FOLLOWING THESE INSTRUCTIONS MAY RESULT IN EXTREME DANGER OF AN ELECTRICAL FIRE.

1. Terminate the upstream S-Net cable at J2 of the power supply. Notice that no connection is made from the upstream shield.
2. Cut supply jumpers J4 and J5.
3. Connect downstream S-Net to J2 of the power supply, connecting the shield to the supply chassis ground.
4. Connect the power fail signals from pins 1 and 2 of J3 to a monitor point as required.

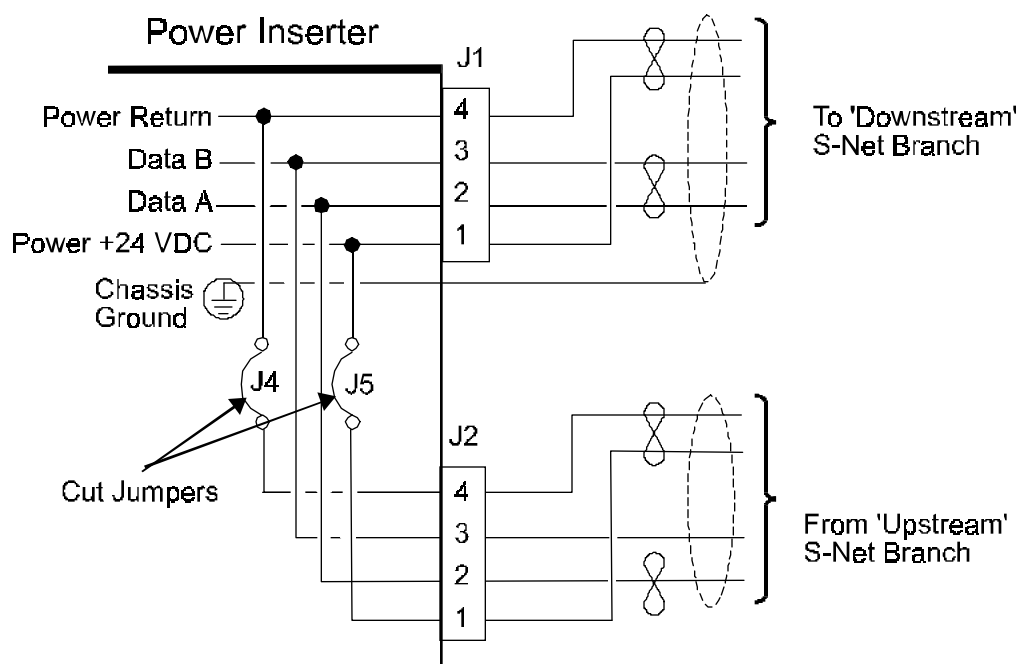


Figure 4-6: Additional Power Inserter Wiring

4.3 RS-485 INTERFACE

All digital readers* and keypads are connected to and controlled by the Alto 818 via the S-Net. S-Net connection to the Alto 818 is through the RS-485 port.

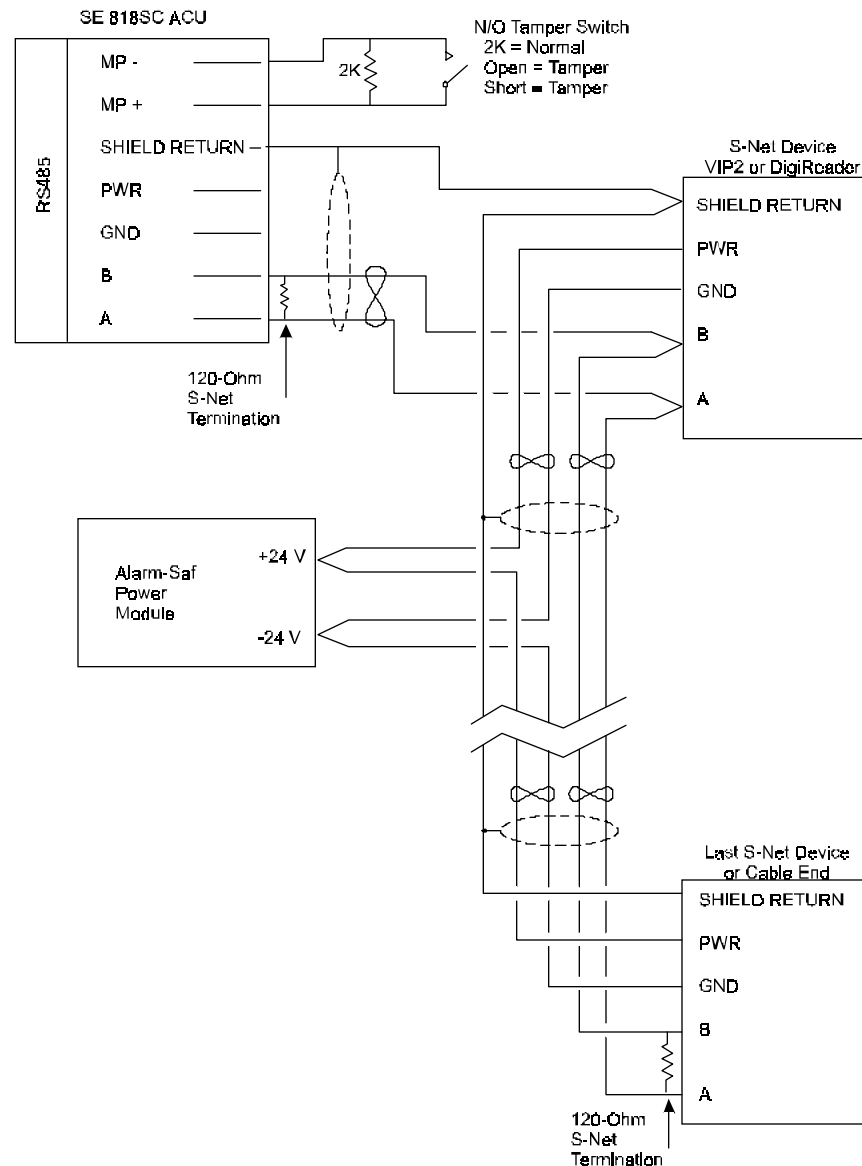


Figure 4-7: RS-485 Interface Wiring for S-Net Devices and Tamper

* The DigiReaders may be used with the SE 818SC only. They are not supported by the SE 818SX.

Connectors labeled SHIELD RETURN, PWR, GND, B and A are used for S-Net connections. The MP+ and the MP- terminals are used for an auxiliary SE 818 tamper input. If this function is not used, a 2K-ohm resistor must be connected across these pins. The system will generate a TAMPER signal at any resistance other than 1520 to 2600 ohms.

All S-Net node devices have a hexadecimal address switch which must be set uniquely as part of the installation procedure. Valid addresses are 1 through 8, hexadecimal. This means that there can be a maximum of 8 readers of a specific type. However, the address numbers may be repeated for a different type of reader, i.e., there may be a digital reader with address 2 and an VIP2 with address 2. The address setting designates the door number in the database.

4.4 ANALOG SENSORS

Analog sensors connect to either a SE 774-A MSM or directly to an Alto 818 reader port via coaxial cable using F-56 connectors. Refer to Section 3.5 for the rules governing the installation of coax cable. Note that the maximum distance for an SE 2814/15 reader from the Alto 818 is 1,000 feet (305 m).

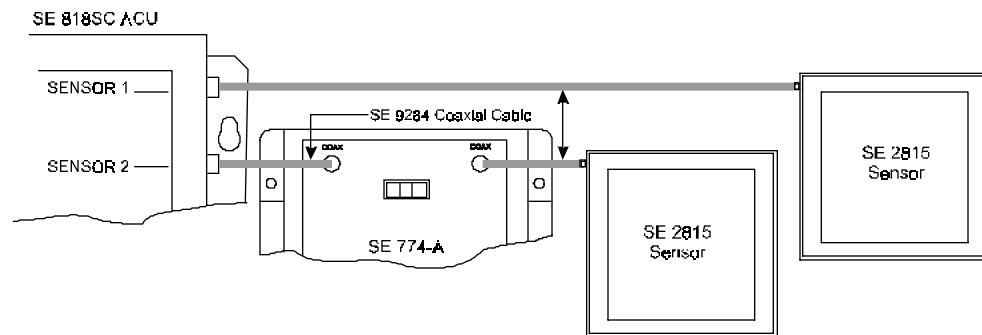


Figure 4-8: Analog Proximity Sensors

Interface wiring for the DigiReaders is discussed in Section 4.3.

4.5 LOCK WIRING INTERFACE

As shown in Figure 4-9, up to eight door locks can be controlled by the Alto 818 via the relays connector.

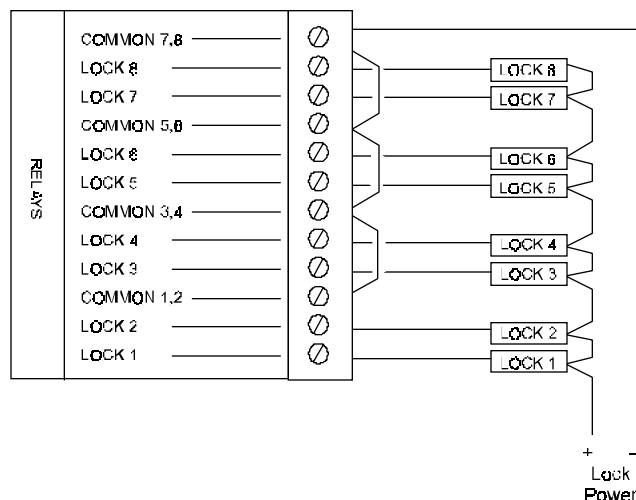


Figure 4-9: Door Lock Interface Wiring

The maximum current each relay contact can carry is 3 amps with an inductive load at 120 VAC. The returns are tied together in pairs (Lock 1, Lock 2 return is 1, 2 Common, etc.). These returns, however, are isolated from the ACU ground. Lock twisted pair wiring must be able to meet the requirements of the National Electrical Code.

Software control, the DOOR command, can be used to configure the system for a reverse lock (closed when power is applied).

4.6 SE 744-A MSM INTERFACE WIRING

Each SE 774-A MSM can be used to interface up to four monitor point contacts and one reader with each reader port on the Alto 818.

4.6.1 READER CONNECTIONS

The SE 774-A MSM is a series connection between a reader and an Alto 818 reader port. The MSM has two female coax connectors for this purpose and it makes no difference which one is used to connect to the reader and which one to the ACU. The MSM counts as one splice in a reader-to-ACU coax cable run. As such, it can be located at any point between the reader and the ACU. The maximum length for this cable run depends upon the reader model (see specifications for the reader).

4.6.2 MONITOR POINT CONNECTIONS

The MSM has four monitor point contact pairs. Monitor points are connected to the MSM with unshielded, twisted pair wires, size AWG 22 or larger. The contact-to-MSM distance can be no more than 200 feet (61m).

The monitor point contacts twisted pair wires connect to a terminal block mounted on the face of the MSM. As shown in Figure 4-10, the method of connection depends upon whether the monitoring contacts are normally open (N/O) contacts or are normally closed (N/C) contacts. For N/O monitoring contacts, a 36K-ohm resistor must be connected in *parallel* with the contacts; for N/C monitoring contacts, a 36K-ohm resistor must be connected in *series* with the contacts.

CAUTION:

A 36K-ohm resistor must be installed across all MSM contact pairs, used or not.

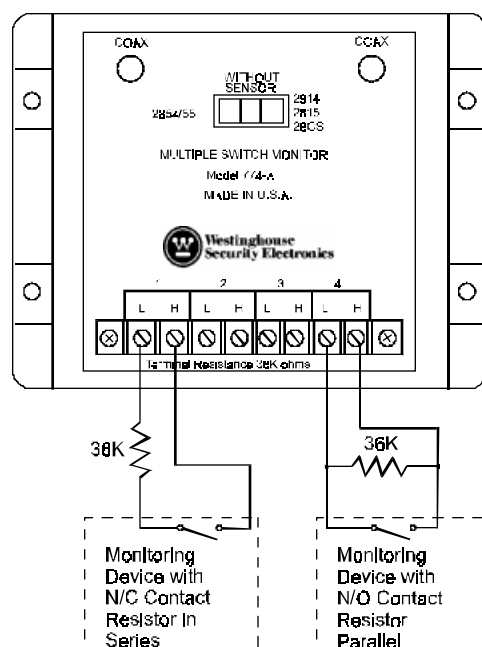


Figure 4-10: MSM Connections for N/O and N/C Monitoring Contacts

4.7 HOST AND SYSTEM TERMINAL INTERFACE WIRING

The host connector and the terminal connector on the Alto 818 provide RS-232C serial data interfaces for a host computer and a terminal, respectively. The Alto 818 software default setup is for an RS-232C null modem terminal interface cable as shown in Figure 4-11. The maximum length of this cable must be held to 25 feet (7.6 M).

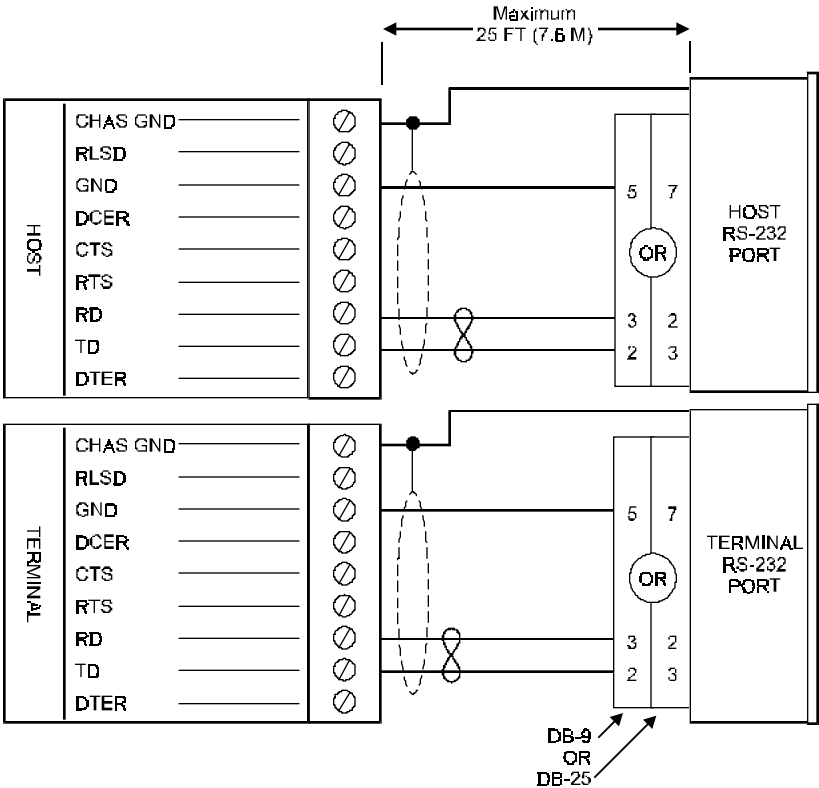


Figure 4-11: Host and Terminal RS-232C Interface Wiring Using a Null Modem Cable

When the Alto 818 is connected to a host system via an HP Terminal Concentrator (model D2040A), the interface cable is shown in Figure 4-12. WSE recommends that this cable not exceed 25 feet (7.6 M) in length.

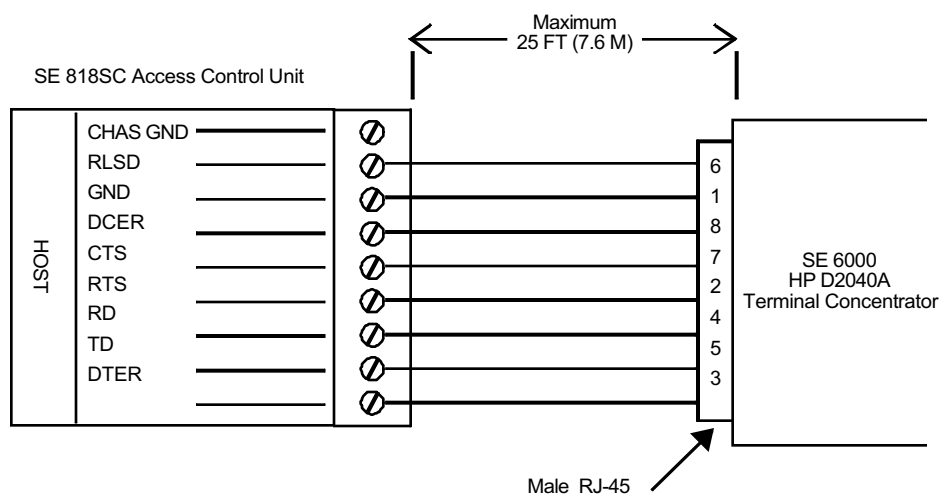


Figure 4-12: SE 6000 System HP Terminal Concentrator (Model D2040A) Interface

4.8 REMOTE TERMINAL WIRING

The host connector on the Alto 818 is a RS-232 serial data port that can be used to connect a local modem to a remote modem via telephone lines. This interface is shown in Figure 4-13. The TX terminals on the local modem are connected to the RX terminals on the remote modem and the local modem RX terminals are connected to the remote modem TX terminals.

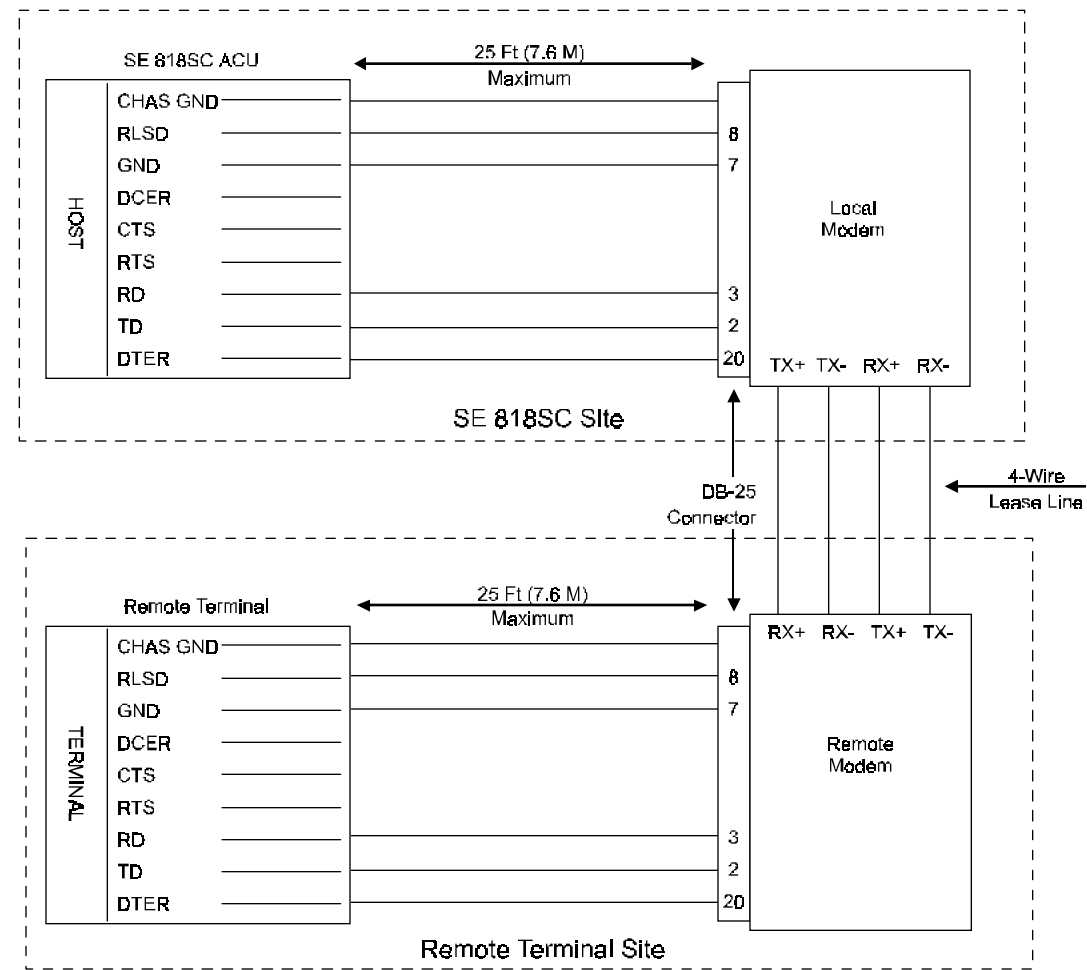


Figure 4-13: Remote Terminal Interface Wiring

4.9 SE 778-A INTERFACE WIRING

The Alto 818 interfaces with the SE 778-A Annunciator/Control panel (Ann/C) by means of a 15-conductor cable which is connected to the annunciator connector on the ACU; see Figure 4-14. The maximum length of this cable is 15 feet (4.4 M).

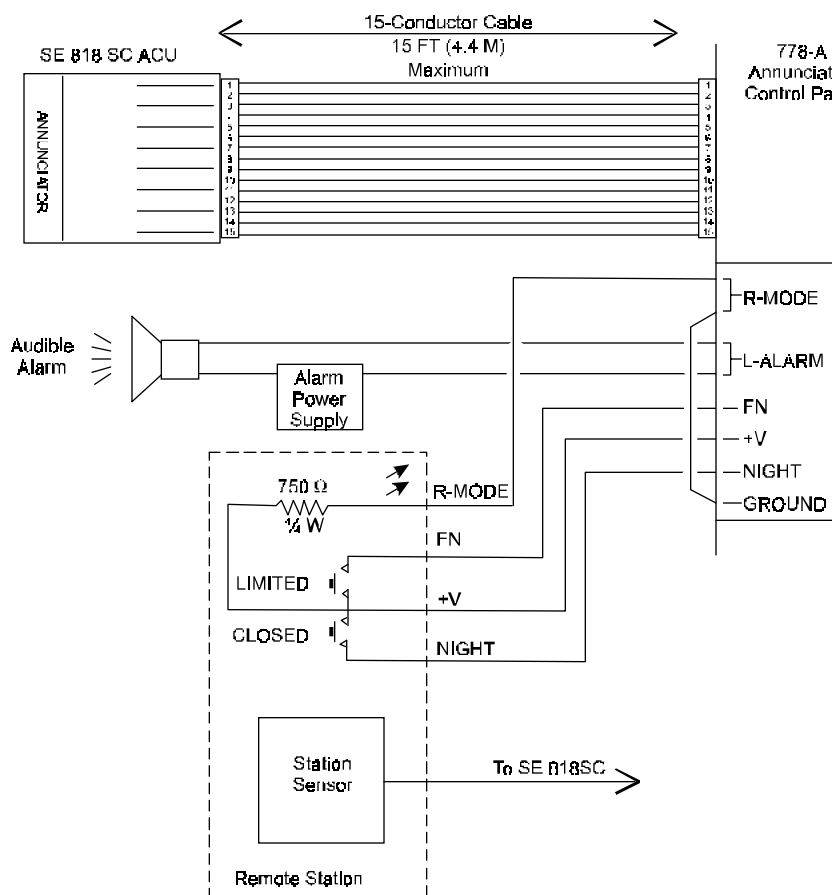


Figure 4-14: SE 778-A Annunciator/Control Panel Interface (with Remote L/C Station)

The terminals labeled L-ALARM on the Ann/C are a set of latched contacts that are typically connected to an audible alarm as shown in Figure 4-14. As programmed by the Alto 818, these contacts will latch closed for a specified alarm condition, causing the alarm to sound. The L-ALARM contacts can only be unlatched by use of the SILENCE command or the RESET command or through a power failure.

4.10 20 mA LOOP WIRING

When a remote terminal is interfaced with the Alto 818 using the 20 mA loop connector, the remote terminal is connected to a CI-1 Communications Interface. The CI-1 is then connected to the 20 mA connector on the Alto 818 as shown in Figure 4-15. The TX terminals on the Alto 818 are connected to the RX terminals at the communications interface device, and the RX terminals are connected to the TX terminals. These connections should be made with #22 AWG (or larger) dual twisted-pair unshielded cable. Use metallic conduit or choose the wiring route to minimize RFI. Avoid fluorescent lighting, high voltage wiring, CB transmitter cable, etc. The maximum recommended wire run is 2,000 feet (610M).

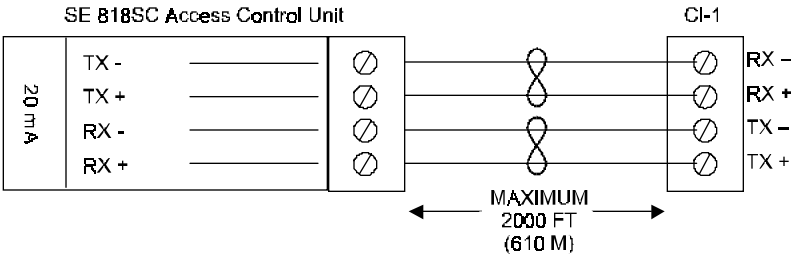


Figure 4-15: 20 mA Interface Wiring

4.11 REMOTE DIAL-UP INTERFACE

Two 6-foot (1.85-meter), 25-pin connector cables are included with the Remote Dial-Up Interface (RDI). These cables provide connection of the RDI between the Alto 818 host port and a modem. All other connections are standard modem connections.

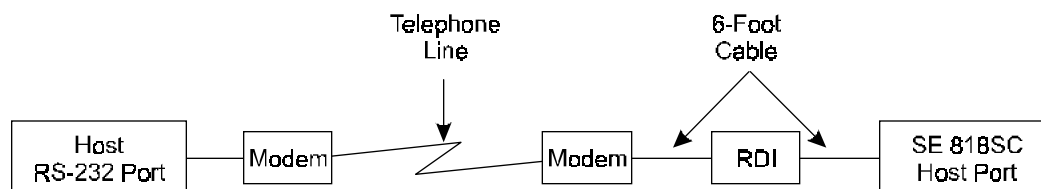


Figure 4-16: Remote Dial-Up Interface Installation

SECTION 5: BENCH CHECK

This section contains the bench check procedures that are recommended before the equipment is placed in service. It is recommended that all tests described should be performed on all Alto 818 ACUs.

The setup procedure is based on a configuration which uses analog sensors, MSMs for monitor points and one or more RS-485 (S-Net) devices. If, however, the intended installation site will not use all of these devices, and they are not otherwise available for the bench test, the associated procedures may be omitted.

5.1 UNPACKING

1. Inspect new equipment before beginning a bench test; report any damage to the carrier and to WSE.
2. Retain the container and protective packing material for use in transporting equipment to the installation site or for return to factory, if required.
3. If a malfunction occurs during the bench check, do not attempt to troubleshoot or repair the equipment; notify WSE immediately.

5.2 TEST SETUP

The required equipment for performing a bench test is listed in Table 5-1.

Description	WSE Product
ACU power supply	SE 3718SU or SE 3708CU
Terminal	SE 57101
S-Net Device	DigiReader or VIP2
S-Net power supply	Alarm-Saf or Power Inserter
Analog sensor	SE 28XX series
Multiple switch monitor	SE 774-A
Coaxial cable with connectors	SE 9284 coax cable
Dual twisted-pair S-Net wire with connectors	
Digital multimeter or ohmmeter	
SPST toggle switch or jumper wire	
36K-ohm resistor	

To set up the ACU for testing and perform power on, proceed as follows:

1. Connect one SPST toggle switch and one 36K-ohm resistor in parallel across one set of terminals on the MSM as shown in Figure 5-1. Ensure that the switch is in the open position. (A wire which can jumper the L and H connectors on the MSM may be substituted for the switch.)

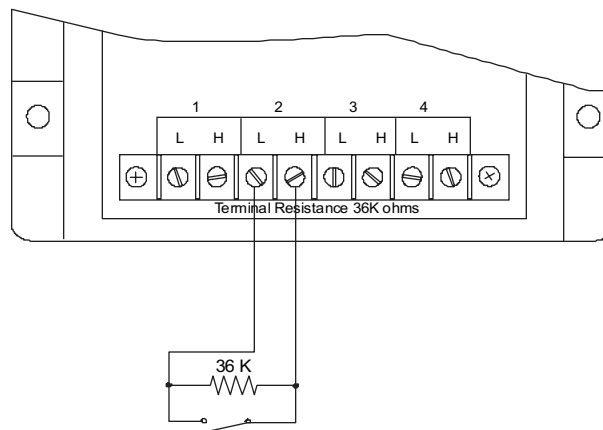


Figure 5-1: MSM Configured for Bench Check

2. Ensure that the AC input switches on the power module and terminal are off, and connect equipment as shown in Figure 5-2.
 - A. Connect the terminal to the terminal port of the ACU as described in Section 4.
 - B. Connect an SE 3708CU or SE 3718SU power module to the power port of the ACU as described in Section 4.
 - C. Connect an SE 28XX sensor to an MSM using SE 9284 coax cable.
 - D. Connect the MSM to Alto 818 ACU sensor 1 port using SE 9284 coax cable. Ensure that the MSM switch on system PCA of the Alto 818 is set for the correct MSM model, and that the MSM switch is set for sensor use.
 - E. Connect a VIP2 keypad or DigiReader to an Alarm-Saf power module and to the ACU RS-485 port.

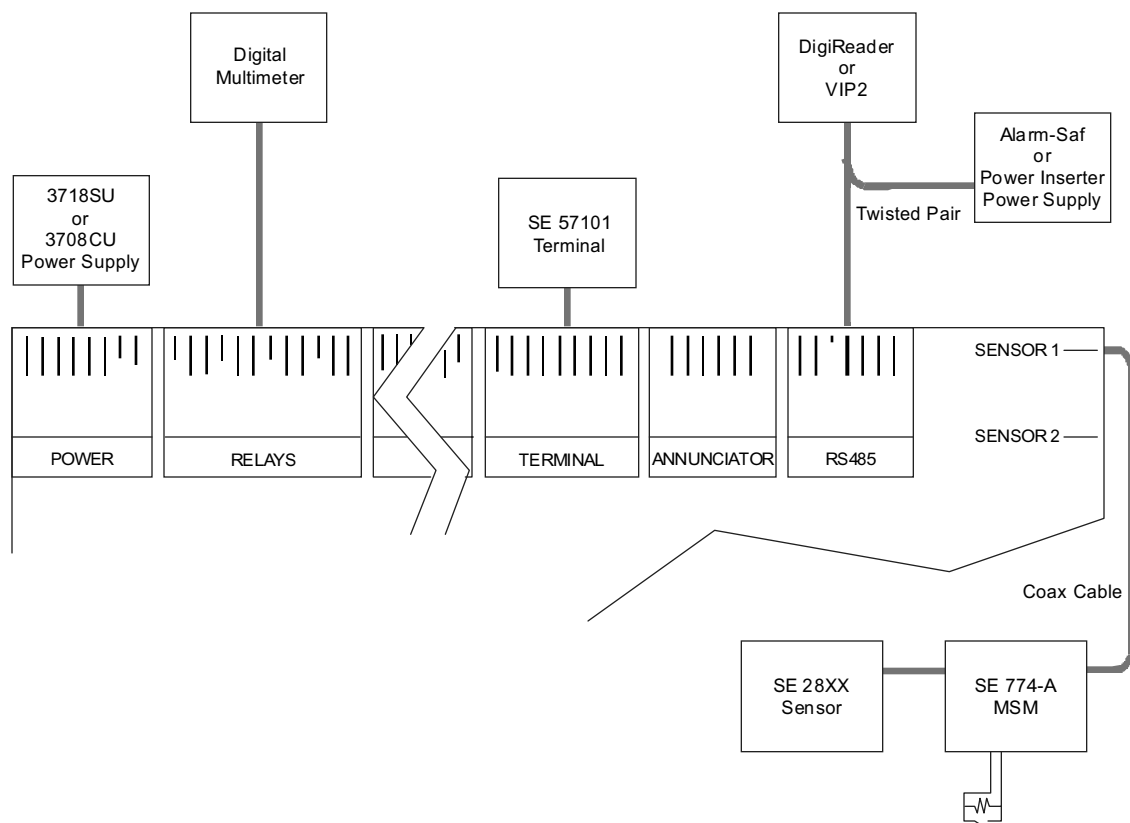


Figure 5-2: Alto 818 Test Setup

3. Turn the terminal on.

4. If using a SE 57101 terminal, reset the terminal setup configuration as follows:

A. Press shift and setup keys simultaneously; the setup menu bar will appear across the bottom of screen.

B. Use the down arrow to scroll through the setup displays; stop at **SET 4**. The display should read:

|SET 4|EIA=HOST|7 BITS|BIT8 1|PARITY ON|PARITY ODD|STOP1|BAUD:300|

C. Use the left and right arrow keys to scroll *horizontally* across the menu; use the space bar to scroll *vertically* at any menu entry that does not read as shown in step 5B, above.

D. Press setup key to return to main screen.

If using a Qume 101-compatible terminal other than an SE 57101, set up the terminal for 7 bits, 1 stop bit, odd parity, and baud rate 300 as described in terminal users manual.

5.3 TEST PROCEDURES

Each Alto 818 undergoes rigorous quality assurance testing before it is shipped from the factory. When a bench test is desirable, the following tests can be used to verify proper operation of the primary input and output connections to the Alto 818.

If the Alto 818 ACU does not perform in the manner indicated in the tests, verify the test setup and components used. If the correct responses are not achieved, return the Alto 818 to the factory.

5.3.1 POWER ON

1. Turn the system power module on.
2. Check that the vital function LED on the Alto 818 is blinking rapidly. If not verify that the power module is correctly installed and powered on.
3. Check that the LED on SE 28XX sensor is on. If not:
 - A. Check that the MSM and sensor are correctly installed.
 - B. Check that the sensor switch on the MSM is set correctly.
 - C. Check that the MSM select switch on the auto sensing board (remove ACU cover to access) is set for the correct MSM type.

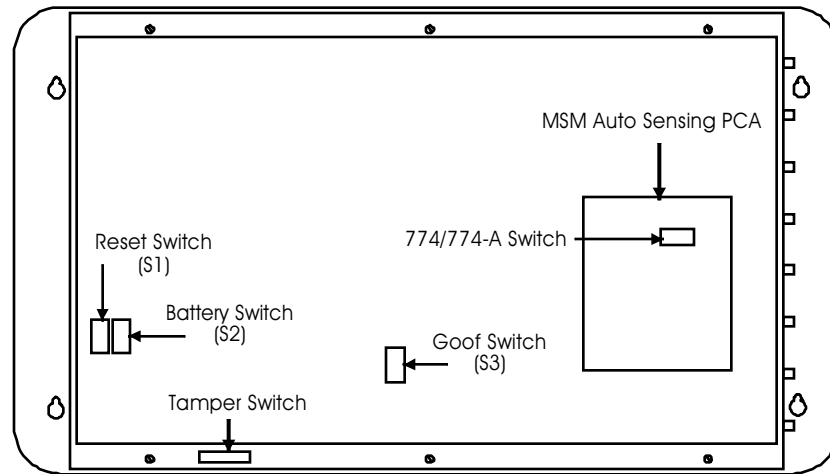


Figure 5-3: Alto 818 Switch Locations (Cover Removed)

5.3.2 TERMINAL TEST

This test is used to verify the installation and configuration of the terminal.

1. Observe the terminal monitor; the screen should display system status. (All times and dates shown are based on factory settings.) If the status is not displayed:
 - A. Verify that the Alto 818 and the terminal are correctly connected.
 - B. Verify that the terminal communications parameters are correctly set as described in Section 5.2.
2. Press the Enter key. The screen displays:

YOUR PASSWORD?
3. Type NEW and press Enter. (The password must be entered within 10 seconds after it is requested.) The screen displays:

HELLO
TYPE HELP FOR A LIST OF COMMANDS
YOUR COMMAND?

5.3.3 LOCK RELAY TEST

This test will verify the operation of the Alto 818 lock relays. Valid abbreviations for commands used are shown in parentheses.

1. Type UNLOCK (UNL) and press Enter. The screen displays:

D00R 1-8 OR 0 FOR ALL)?

2. Type 0 and press Enter. Listen for the “click” of relays and observe that all green relay LEDs illuminate in sequence on the ACU.
3. Set the DMM, or ohmmeter, on the 10-ohm scale. Measure the resistance between each lock terminal (lock 1 through lock 8) and its associated common terminal. The meter should read 0 ohms resistance. If the meter reading indicates any resistance or an open circuit (infinite resistance) for any lock terminal, that lock relay is not functioning properly and unit should be returned to the factory.

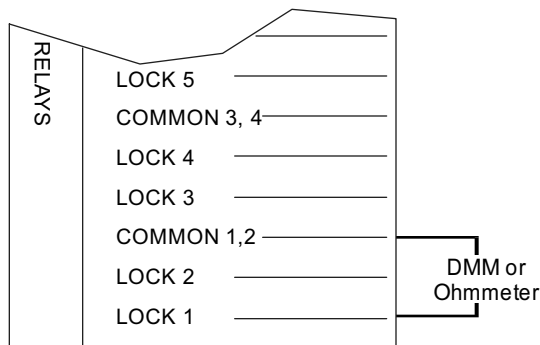


Figure 5-4: Measuring Lock Relay Resistance

4. At the command prompt, type RELOCK (REL) and press Enter; the screen displays:

D00R (1-8 OR 0 FOR ALL)?

5. Type 0 and press Enter; listen for the “click” of relays and observe that all green RELAY LEDs go out in sequence.
6. Repeat resistance measurements in step 3, above; all relay contacts should indicate an open line or infinite resistance. If the meter reading indicates zero or any resistance on the 10-ohm scale for any lock terminal, that lock relay is not functioning properly and unit should be returned to the factory.

5.3.4 MONITOR INPUT TEST

This test will verify the monitor input functions of the Alto 818.

1. Exit the command mode by typing BYE (B) at the command prompt.
2. Using the toggle switch installed on the MSM as in Figure 5-1, close the contact. If a jumper wire is used, short the L and H contacts on the MSM. The terminal monitor should indicate an active relay point with a message similar to:

40 16:23:22 (1.2) MONITOR POINT ACTIVE

Alternately, log in, enter the command mode and type STATUS (STA) at the prompt to display the monitor point status. The terminal should display the status similar to:

Building Mode		Tamper		Power		Alarm					
-----0-----		-----A---		-----		-----					
#####	Door	Coax	SnSr	Reader	VIP	MSM	MP1	MP2	MP3	MP4	
--#1--	-----	-----	-----	---NE---	---NE---	-----	-----	---A---	-----	-----	
--#2--	-----	-----	---NE---	---NE---	-----	---NE-	-----	-----	-----	-----	
--#3--	-----	-----	---NE---	-----	---NE---	---NE-	-----	-----	-----	-----	
--#4--	-----	-----	---NE---	---NE---	---NE---	---NE-	-----	-----	-----	-----	
--#5--	-----	-----	---NE---	---NE---	---NE---	---NE-	-----	-----	-----	-----	
--#6--	-----	-----	---NE---	---NE---	---NE---	---NE-	-----	-----	-----	-----	
--#7--	-----	-----	---NE---	---NE---	---NE---	---NE-	-----	-----	-----	-----	
--#8--	-----	-----	---NE---	---NE---	---NE---	---NE-	-----	-----	-----	-----	

O = Open L = Limited C = Closed
 F = Fail S = Shunted A = Active U = Normal Unlock NE = Not Enabled
 HO = Held Open Fo = Forced Open TS = Tamper Shunted TA = Tamper Active

Figure 5-5: STATUS Display — Monitor Point 1.2 Active

3. Open the toggle switch, or remove wire used to short the contacts. The terminal monitor should indicate that the monitor point is not clear; a message should be displayed similar to:

41 16:24:01 (1.2) MONITOR POINT CLEAR

Repeat this test on all sensor ports as required.

5.3.5 SENSOR TEST

With an SE 28XX sensor connected to an Alto 818 port as shown in Figure 5-2 (MSM not required), verify sensor operation with the following procedure.

1. From the command prompt, type DOOR (DO) and press Enter.
2. Enter the door number which corresponds to the sensor port (door).
3. Type 8 and press Enter. The screen displays:

8A. SENSOR ENABLE (Y/N) : N?
4. Type Y and press Enter.
5. Press the Escape key to exit the command.
6. At the command prompt, type STATUS (STA) to display the status of the sensor on the door defined above. The correct display for a sensor on door 1, a DigiReader on door 3 and VIP2 on door 2 are highlighted on the sample STATUS screen, Figure 5-5.

The sensor LED should be illuminated.

5.3.6 RS-485 (S-NET) TEST

Testing of the RS-485 functions of the Alto 818 require the use of an S-Net device. This device may be a VIP2 keypad or a DigiReader digital command key reader. The DOOR command will be used to enable the S-Net devices.

DIGIREADER*

1. From the command prompt, type DOOR (DO) and press Enter.
2. Enter the door number which corresponds to the address of the DigiReader.
3. Type 8 and press Enter; press Enter again to display prompt line 8C as shown below.

8C. SNET READER TYPE (NONE/DKR/SCR) : DKR?

4. Press the Escape key to exit the command.

* Perform this test when DigiReaders are installed on an SE 818SC only. DigiReaders are not supported by the SE 818SX.

- At the command prompt, type STATUS (STA) to display the status of the digital reader on the door defined above. The correct display for a sensor on door 1, a DigiReader on door 3 and VIP2 on door 2 are highlighted on the sample STATUS screen, Figure 5-6.

The DigiReader LED should be illuminated.

VIP2

- From the command prompt, type DOOR (DO) and press Enter.
- Enter the door number which corresponds to the address of the VIP and press Enter.
- Type 19 and press Enter. The screen will display:

19. VIP ENABLE (Y/N) : N?
- Type Y and press Enter.
- Press the Escape key to exit the command.
- At the command prompt, type STATUS (STA) to display the status of the VIP2 on the door defined above. The correct display for a sensor on door 1, a DigiReader on door 3 and VIP2 on door 2 are highlighted on the sample STATUS screen, Figure 5-5

The middle VIP2 LED should be illuminated.

Building Mode		Tamper	Power	Alarm
-----0-----		----A----	-----	-----

#####	Door	Coax	SnSr	Reader	VIP	MSM	MP1	MP2	MP3	MP4
--#1--	-----	-----	-----	----NE--	----NE--	-----	-----	-----	-----	-----
--#2--	-----	-----	--NE--	----NE--	-----	--NE-	-----	-----	-----	-----
--#3--	-----	-----	--NE--	----NE--	----NE--	--NE-	-----	-----	-----	-----
--#4--	-----	-----	--NE--	----NE--	----NE--	--NE-	-----	-----	-----	-----
--#5--	-----	-----	--NE--	----NE--	----NE--	--NE-	-----	-----	-----	-----
--#6--	-----	-----	--NE--	----NE--	----NE--	--NE-	-----	-----	-----	-----
--#7--	-----	-----	--NE--	----NE--	----NE--	--NE-	-----	-----	-----	-----
--#8--	-----	-----	--NE--	----NE--	----NE--	--NE-	-----	-----	-----	-----

O = Open L = Limited C = Closed
 F = Fail S = Shunted A = Active U = Normal Unlock NE = Not Enabled
 HO = Held Open Fo = Forced Open TS = Tamper Shunted TA = Tamper Active

Figure 5-6: STATUS Display — Sensor, DigiReader and VIP2

5.3.7 BENCH CHECK CONCLUSION

To conclude the bench check, proceed as follows:

1. If still in the command mode, type BYE (B); and press Enter.
2. Turn the ACU power module off. Turn off the power module used for the RS-485 S-Net devices.
3. Disconnect all cables and wiring from the Alto 818.
4. If you do not plan immediate installation of the ACU, remove the cover from the Alto 818 and ensure that S2 (Figure 5-3) is off. Replace the cover of the Alto 818.
5. Repack the Alto 818 in the original shipping container using the same packing method and materials used by the factory.

SECTION 6: COMMANDS

This section describes the system commands as entered from the keyboard of a terminal or a computer emulating a terminal. The commands are listed in alphabetical order.

Instructions for configuring the Alto 818 using the commands are discussed in Section 7; operation instructions are covered in Section 8. For configuration and operation from a host, see the appropriate security management system manual.

6.1 KEYBOARD ENTRIES

Entries may be made to the Alto 818 database and operation commands issued from a host computer or from a terminal keyboard. This subsection describes keyboard techniques which are valid for command entry from either.

A host computer operation is provided through an SE 5850, SE 6000 or NexSentry Manager security management system (SMS). An entire database may be downloaded to the Alto 818 via a modem, or a single command can be issued. See the appropriate SMS manual for further details.

6.1.1 DAYS AND DATES

Below are system abbreviations and valid keyboard entries for the indicated days and months.

Day	Display	Minimum Keyboard Entry
Sunday	SUN	SU
Monday	MON	M
Tuesday	TUE	TU
Wednesday	WED	W
Thursday	THU	TH
Friday	FRI	F
Saturday	SAT	SA
Holiday	HOL	H

Month	Display	Minimum Keyboard Entry
January	JAN	JA
February	FEB	F
March	MAR	MAR
April	APR	AP
May	MAY	MAY
June	JUN	JUN
July	JUL	JUL
August	AUG	AU
September	SEP	S
October	OCT	O
November	NOV	N
December	DEC	D

When entering dates or years, leading zeroes are not significant. Entering 1-F-1 will result in the date 01-FEB-01.

Displayed date fields are interpreted as follows:

DD-MMM-YY where:

DD = Two-digit number for day of the month (for days 1 through 9, a 0 will precede the number)

MMM = Month of the year (JAN, FEB, MAR, APR, MAY, etc.)

YY = Last two digits of the year (96, 97, 98, etc.)

For example, if a holiday is to be scheduled for July 4, 1999, this date would be displayed as:

04 JUL 99

You may use a number of delimiters between the day, month and year fields. Thus, all the following would be valid entries for 4 SEP 96

**4 S 96
04 , S , 96
04 . S . 96
4 : SEP : 96
04-SEP-96**

6.1.2 TIME ENTRIES

Each displayed time entry consists of both hour and minute values appearing in the format 08:00, the hour separated from the minutes with a colon. All entries are based on a 24-hour clock, 00:00 being exactly midnight (to begin the specified date). As when entering dates, the same delimiters may be used when entering a time. The following would be valid entries for 9:35 am:

**9 35
09 : 35
9 - 35
09 , 35
09 . 35**

Because a 24-hour clock is used, 9:35 pm could be entered as:

**21 35
21 : 35
21 - 35
21 , 35
21 . 35**

Time intervals are displayed by the system as follows: 00:00-00:00. A time interval between 5:30 PM of one day and 1:30 AM on the next day is displayed as 17:30-01:30. Using different delimiters, possible entries are:

```
17 30 1 30
17:30-01:30
17,30-1.30
```

Leading zeroes do not need to be entered.

NOTE:

Time interval entries must include days as well as start and stop times.

6.1.3 ENTER KEY

When data for a given field in a command is typed on the system keyboard, this data will be stored in the Alto 818 memory as soon as the Enter key is pressed. The data will be entered even if there are other fields in the command that require additional data to be entered.

6.1.4 ESCAPE (ESC) KEY

Exit from a command at any point by pressing the Escape (ESC) key. (Check the manual for the terminal you are using to determine the equivalent function key.) If a command is interrupted in this manner, all of the data entered (Enter key pressed) with that command prior to pressing the ESC key will be retained in memory.

6.2 COMMAND TYPES

Commands can be divided into three categories:

- Operation** Commands which may be used during normal operation of the access control system.
- Database** Commands used to make entries to the Alto 818 database. Database commands are used prior to initial operation of the Alto 818 for access control, and later to make modifications to the database as required.
- Print** The PRINT command is used in combination with the other commands to display the current configuration.

All system commands, arranged by category are shown in Table 6-1.

Table 6-1: Command Categories

Operating Commands				
BYE	CLOSE	HELP	LIMIT	OPEN
PRINT	RELOCK	SILENCE	SHUNT	STATUS
UNLOCK	UNSHUNT	VERSION		

Database Commands				
ACCESS	DELETE	DOOR	GROUP	FORGIVE
HOLIDAY	KEY	MODEM	MONITOR	REPORT
SYSTEM	TIME	USER	XLOAD	XSAVE

Print Command Choices				
ACCESS	DOOR	HOLIDAY	KEY	MODEM
MONITOR	REPORT	SYSTEM	TIME	USER

6.3 COMMAND DESCRIPTIONS

In the command mode, after a valid password has been entered, entering HELP will cause the list of all commands to be displayed. Commands can be abbreviated as shown in Table 6-2.

During database setup, one of six user authorization ranks, rank A through F, is assigned to each user. Thereafter, the availability of any command to any user depends on the rank to which they have been assigned. The table below lists all commands, valid keyboard abbreviations and user authorization ranks.

Table 6-2: Command Ranks

Command	Abbreviation	Authorization Rank					
		A	B	C	D	E	F
ACCESS	A	X	X				X
BYE	B	X	X	X	X	X	X
CLOSE	C	X	X	X	X		
DELETE	DE	X	X				X
DOOR	DO	X					
FORGIVE	F	X	X	X			
GROUP	G	X	X				
HELP	HEL	X	X	X	X	X	X
HOLIDAY	HO	X	X				X
KEY	K	X	X				X
LIMIT	L	X	X	X	X		
MODEM	MOD	X					
MONITOR	MON	X					
OPEN	O	X	X	X	X		
PRINT	P	Command Dependent					

Command	Abbreviation	Authorization Rank					
		A	B	C	D	E	F
RELOCK	REL	X	X	X			
REPORT	REP	X					
RESET	RES	X					
SHUNT	SH	X	X	X			
SILENCE	SI	X	X	X	X	X	
STATUS	ST	X	X	X	X	X	
SYSTEM	SY	X					
TIME	TIM	X	X	X			
UNLOCK	UNL	X	X	X			
UNSHUNT	UNS	X	X	X			
USER	US	X					
VERSION	V	X	X	X	X	X	X
XLOAD	XL	X					
XSAVE	XS	X					

Many commands consist of multiple lines for entering parameters. They will normally be numbered in sequential order. The exception is when the selection of a parameter creates additional entries or obviates the need for other entries.

6.3.1 ACCESS

Access codes determine when a command key holder or VIP2 user may access defined doors. The default prompts for the ACCESS command, access code 1, are shown in Figure 6-1. There are 120 available code numbers. An ACCESS setup sheet can be found in Appendix B.

```

ACCESS CODE (1-120)? 1
DOOR (1-8) 1?
(1)
00:00-24:00 SUN MON TUE WED THU FRI SAT HOL ?
00:00-00:00 ?
00:00-00:00 ?
00:00-00:00 ?
(2)
00:00-24:00 SUN MON TUE WED THU FRI SAT HOL ?
00:00-00:00 ?
00:00-00:00 ?
00:00-00:00 ?
(3)
00:00-24:00 SUN MON TUE WED THU FRI SAT HOL ?
00:00-00:00 ?
00:00-00:00 ?
00:00-00:00 ?
(4)
00:00-00:00 SUN MON TUE WED THU FRI SAT HOL ?
00:00-00:00 ?
00:00-00:00 ?
00:00-00:00 ?
(5)
00:00-24:00 SUN MON TUE WED THU FRI SAT HOL ?
00:00-00:00 ?
00:00-00:00 ?
00:00-00:00 ?
(6)
00:00-00:00 SUN MON TUE WED THU FRI SAT HOL ?
00:00-00:00 ?
00:00-00:00 ?
00:00-00:00 ?..
(7)
00:00-00:00 SUN MON TUE WED THU FRI SAT HOL ?
00:00-00:00 ?
00:00-00:00 ?
00:00-00:00 ?
(8)
00:00-00:00 SUN MON TUE WED THU FRI SAT HOL ?
00:00-00:00 ?
00:00-00:00 ?
00:00-00:00 ?

```

Figure 6-1: ACCESS Command Prompts

Access code 1 is preprogrammed at the factory to be applicable to all controlled doors, 24 hours a day, 7 days a week, including holidays. It is useful when the system is first installed on site, before the database is set up. The access doors and times for code 1 can be changed during or after database setup to suit the requirements of the installation.

The remaining access codes (2-120) have no preprogrammed time intervals or days for any door.

To enter access code data, proceed as follows:

1. At the command prompt, type ACC and press Enter. The screen displays:

ACCESS CODE (1-120)?

2. Accept this code number or type a different number and press Enter. The screen displays:

DOOR (1-8)?

3. Enter the desired door number or make no entry for door 1. Press Enter. The screen displays

**(1)
00:00-00:00**

4. Enter the time intervals and days for access to door 1. The time/day prompt is repeated three times for a total of four time intervals. Press Enter after the fourth interval. The screen displays:

**(2)
00:00-24:00 ?**

5. Continue to enter time intervals and days for the remaining doors, 2 through 8, as required.

6.3.2 BYE

The BYE command is used by an operator to log off the system and to return to the operation mode. A valid password must be entered to again enter the command mode.

6.3.3 CLOSE

This command is applicable only if the Alto 818 system is set up to use building modes, and open, closed and station sensors have been defined with the DOOR command (see Section 6.3.5). Entering the CLOSE command places the building in the building-closed mode.

6.3.4 DELETE

The DELETE command is used to delete key holder codes from the database. This command should be used judiciously. For security reasons, it is often advisable to change a key holder's access code to **0** instead of deleting the key code (see Section 6.3.10).

When **DEL** is entered in response to the **YOUR COMMAND?** prompt, the screen display is:

```
YOUR COMMAND? DEL
KEY CODE?
```

Type in the code of the key you wish to delete and press Enter. The key code will be deleted automatically and screen will again display the command prompt. If the key with the code you enter is not already in the system database, screen will display:

```
YOUR COMMAND? DEL
1050/1060 KEY (Y/N)? Y

KEY CODE? 123456

NOT IN MEMORY
```

You can check that the key code was deleted by entering its code a second time with the DEL command. If the **NOT IN MEMORY** statement is displayed the second time the key code is entered, you have verified its deletion.

6.3.5 DOOR

The DOOR command is used to specify which readers are associated with a given door, to define the door monitoring devices (i.e., door switches, REXs, readers), to assign any reports that are associated with door activity, to specify and define anti-passback control, to enable and define a VIP2 keypad if one is used, and to define various other door control functions.

Make the appropriate number of copies of the DOOR command setup sheets in Appendix B, fill out these sheets, and then use the DOOR command to enter the data for each of the eight possible door addresses.

1. From the **YOUR COMMAND?** prompt, type **DO** and press Enter. The screen displays:

```
DOOR (1-8) ?
```

2. Type in the desired door number and press Enter. The screen displays

```
GO TO (1-20)?
```

```

DOOR (1-8)?
GO TO (1-20)?
1. NAME (24): ?
2. KEY TRACE REPORT (0-32): 1?
3. ACCESS GRANTED REPORT (0-32): 1?
4. ACCESS DENIED REPORT (0-32): 1?
5. DOOR OPEN TOO LONG REPORT (0-32): 1?
6. DOOR FORCED OPEN REPORT (0-32): 1?
7. COAX FAIL REPORT (0-32): 1?
8. SELECT READER TYPE
8A. SENSOR ENABLE (Y/N): Y?
8B. SENSOR FAIL REPORT (0-32): 1?
8C. SNET READER TYPE (NONE/DKR/SCR): DKR?
8D. SNET READER FAIL REPORT (0-32): 1?
8E. DIGITAL KEY READER RANGE (0-255): 254?
9. MSM ENABLE (Y/N): Y?
9A. MSM FAIL REPORT (0-32): 1?
10. SENSOR TYPE (NORMAL/OPEN/CLOSED/STATION): NORMAL?
11. ANTI-PASSBACK (NONE/ENTRY/EXIT): ENTRY?
11A. TYPE (HARD/SOFT): HARD?
12. REVERSE LOCK (Y/N): N?
13. UNLOCK TIME (1-240): 10?
14. DOOR OPEN TOO LONG TIME (1-240): 10?
15. DOOR SWITCH (X.Y): ?
16. REX SWITCH (X.Y): ? 3.2
16A. UNLOCK ON REX (Y/N): N?
16B. VALID REX
    00:00-00:00 ?
    00:00-00:00 ?
    00:00-00:00 ?
    00:00-00:00 ?
16C. EXIT GRANTED REPORT (0-32): 1?
16D. EXIT DENIED REPORT (0-32): 1?
17. AUTO UNLOCK
    00:00-00:00 ?
    00:00-00:00 ?
    00:00-00:00 ?
    00:00-00:00 ?
18. READ KEY WHILE DOOR IS OPEN (Y/N.): N?
19. VIP ENABLE (Y/N): Y?
19A. VIP REQUIRED WHEN BUILDING IS:
    OPEN (Y/N): N?
    LIMITED (Y/N): N?
    CLOSED (Y/N): N?
    AND DURING TIMES AND DAYS
    00:00-24:00 MON TUE WED THU FRI SAT HOL
    00:00-00:00
    00:00-00:00
    00:00-00:00
19B. VIP FAILURE REPORT (0-32): 1?
20. DEVICE TAMPER REPORT (0-32): 1?
    
```

Figure 6-2: DOOR Command Prompts

3. At this time, you may select to jump to any of the available fields by typing the number and pressing Enter. For the default 1, the screen displays:

1. NAME (24) : ?

4. Type a name with a maximum of 24 characters. Descriptive names such as FRONT LOBBY or DELIVERY ENTRANCE are advised. Press Enter.
5. The screen displays:

2. KEY TRACE REPORT (0-32) : 1?

Prompt 2 is the first of several fields which allow you to assign a report number to various door activities. If any of the log events do not require a report, enter 0. All log events in the DOOR command prompts are factory set to report 1.

The key trace function may be enabled for individual users with the KEY command or for a number of users with the GROUP command. Field 2 assigns a report to key trace actions.

3. ACCESS GRANTED REPORT (0-32) : 1?

4. ACCESS DENIED REPORT (0-32) : 1?

Access granted or denied reports are enabled for the specified door by entering a number in fields 3 and 4. A log message is generated each time a command key is presented to a proximity reader or a PIN is entered on a VIP2 associated with the door. (Door functions can be disabled with the SHUNT command. See Section 6.3.18.

5. DOOR OPEN TOO LONG REPORT (0-32) : 1?

This report is generated when the door open time period specified in field 13 below is exceeded.

6. DOOR FORCED OPEN REPORT (0-32) : 1?

A door is considered forced open when no access or exit granted is pending. A request-to-exit (REX) switch can be used to signal a valid door opening; see field 15 below.

7. COAX FAIL REPORT (0-32) : 1?

A failure to the coaxial cable associated with the door, sensor port, will generate this report. A cable short is an example of a coaxial failure.

6. Press Enter after selecting each report number for fields 2 though 7. The screen displays:

8. SELECT READER TYPE

8A. SENSOR ENABLE (Y/N) : Y?

7. Set the SENSOR ENABLE field to Y if an analog proximity sensor will be used on this door (sensor port). If N is entered field 8B is skipped. For a Y response, the screen displays:

8B. SENSOR FAIL REPORT (0-32) : 1?

8. Select a report, 0–32, for a failure of the analog sensor. Press Enter. The screen displays:

8C. SNET READER TYPE (NONE/DKR/SCR) : DKR?

9. If an S-Net device, other than a VIP2, is to be used for this door, enter DKR for a digital reader or SCR for an AT&T Smart Card reader. For no S-Net device, enter NONE. Press Enter. For entries other than NONE, the screen displays:

8D. SNET READER FAIL REPORT (0-32) : 1?

10. Designate a report to be associated with a failure of the above specified S-Net device. Type a number, 0–32 and press Enter. If DKR was input for field 8C, the screen displays:

8E. DIGITAL KEY READER RANGE (0-255) : 254?

11. See the appropriate digital reader manual for details on the read range. Type the desired value and press Enter. The screen displays:

9. MSM ENABLE (Y/N) : Y?

12. Enter Y if an MSM is connected to this door, sensor port; otherwise type N. Press Enter. For a Y entry, the screen displays:

9A. MSM FAIL REPORT (0-32) : 1?

13. Select a report number to be associated with an MSM failure, 0 for no report, and press Enter. The screen displays:

10. SENSOR TYPE (NORMAL/OPEN/CLOSED/STATION) : NORMAL?

14. The sensor type refers to any proximity sensor, analog or digital, or VIP2. The sensor type is only valid when building modes are utilized. Select a type and press Enter. The screen displays:

11. ANTI-PASSBACK (NONE/ENTRY/EXIT) : ENTRY?

15. If anti-passback control is to be used, each door must be designated as an entry or an exit.

When enabled, a valid entry sets the user's location as IN. A valid exit sets the user's location as out. An attempt to enter while a user's location is set to in constitutes a passback violation. Similarly, an exit request while out is a violation. Make a selection and press Enter. When ENTRY or EXIT is entered for field 11, the screen displays:

11A. TYPE (HARD/SOFT) : HARD?

16. Hard anti-passback will not grant access and will generate as anti-passback log message. Soft anti-passback will allow access while generating an anti-passback log message. Type H for hard or S for soft. Press Enter. The screen displays:

* Prompts 8C through 8E are valid only on an SE 818SC.

12. REVERSE LOCK (Y/N) : N?

17. This field makes possible the use of either a fail-safe (unlocks on loss of power) or fail-secure (locks on loss of power) door locks in a system. A fail-safe lock will unlock when lock contacts are opened by the Alto 818 or when power to the ACU is lost. Operation of a fail-secure lock is opposite: The door will be locked when power to the ACU is lost or when the ACU lock contacts are open. Type Y or N as required and press Enter. The screen displays:

13. UNLOCK TIME (1-240) : 10?

18. In field 13, the length of time a door will remain unlocked after a valid access is granted is designated. Enter a time, from 1 to 240 seconds, the default is 10, and press Enter. The screen displays:

14. DOOR OPEN TOO LONG TIME (1-240) : 10?

19. This field is used to select a time period between 1 and 240 seconds during which the door may be held open before a DOOR OPEN TOO LONG log event is recorded. (The door open must be valid.) The default setting for this field is 10 seconds. Type the number of seconds desired and press Enter. The screen displays:

15. DOOR SWITCH (X.Y) : ?

20. A door switch indicates that a door is open. The switch is interfaced to the ACU through a contact pair on an MSM. The monitor point address for a contact pair is defined as X.Y, where:

X = MSM number (sensor port 1–8 to which it is connected)
Y = Number of the MSM contact pair (1-4)

No door switch is represented by 0.0. Enter the desired switch number and press Enter. The screen displays:

16. REX SWITCH (X.Y) : ?

NOTE:

If both a REX switch and a door switch are assigned to a door, the REX switch should be connected to a lower number contact pair than the door switch, i.e., REX switch 3.1 and door switch 3.2.

21. A request-to-exit (REX) switch may be interfaced to the ACU through a contact pair on an MSM. See the above discussion for the door switch. Enter the desired switch number and press Enter. For non 0.0 entries, the additional REX configuration screens are displayed:

16A. UNLOCK ON REX (Y/N) : N?

22. If an N, the default, is selected for this function, the door switch will be shunted upon a valid exit request but the door will not be unlocked. This function should be enabled, enter Y, for doors with a door or lock which must be powered to open. After entering a response, the screen displays:

16B. VALID REX
00:00-00:00 ?

23. Four time intervals are available to schedule when signals from a REX device associated with a given door will be valid. Enter times and days as required and press Enter. The screen displays:

16C. EXIT GRANTED REPORT (0-32) : 1?

24. Specify a report number to be associated with an exit granted action. Enter a number and press Enter. The screen displays:

16D. EXIT DENIED REPORT (0-32) : 1?

25. Specify a report number to be associated with an exit denied action. Enter a number and press Enter. The screen displays:

17. AUTO UNLOCK
00:00-00:00 ?

26. Four time intervals may be selected during which doors are automatically unlocked by the Alto 818. Enable this function for doors that do not required access control during fixed time intervals.

If a door with an OPEN, CLOSED, or STATION sensor is scheduled to unlock during an auto unlock time interval that occurs when the building is in the OPEN mode, it will relock when the building enters the LIMITED or CLOSED modes regardless of the time intervals scheduled. A door with a NORMAL sensor will remain unlocked under these conditions. When an automatic unlock time interval begins and ends, a data log is sent to both the local terminal and to the host port.

Make time and day entries as required. Press Enter. The screen displays:

18. READ KEY WHILE DOOR IS OPEN (Y/N.) : N?

27. This field should be enabled for situations where time-and-attendance are recorded through a host system, such as a door used by employees to enter and exit.

CAUTION:

The use of this function can allow unauthorized individuals to enter the building if the door is not visually monitored by security personnel.

When Y is entered at the prompt, the key reader will remain active and the unlock time will automatically drop to 1 second while the door is open. As long as keys are presented to the sensor within the DOOR OPEN TOO LONG time selected in field 14, no log message will be generated.

It is recommended that time-and-attendance doors be equipped with an audible and/or visual device that activates each time the door is unlocked. Then, if the unlock time is dropped to 1 second, the key holders can tell that their keys has been read as they enter or exit. Such devices will also assist security personnel in monitoring the door.

The default for this prompt is N. Enable as required and press Enter. The screen displays:

19. VIP ENABLE (Y/N) : Y?

28. A VIP2 used on a door must be enabled by a Y response to this prompt; the default is N. Enable or disable the VIP2 for this door as required. When enabled additional parameters may be set; the screen displays:

**19A. VIP REQUIRED WHEN BUILDING IS:
OPEN (Y/N) : N?**

29. When building modes are used, use this field to specify during which modes the VIP2 is required. Select Y or N for this and the two modes to follow. The screen displays:

**LIMITED (Y/N) : N?
CLOSED (Y/N) : N?
AND DURING TIMES AND DAYS
00:00-24:00 MON TUE WED THU FRI SAT HOL**

30. Required times for the VIP can be specified by time and day instead of or in addition to the modes described above. Four time intervals may be entered. Notice the default for the first interval makes the VIP2 required 24 hours a day, every day. Make time and day entries. The screen displays:

19B. VIP FAILURE REPORT (0-32) : 1?

31. Type a report number to be associated with a VIP2 failure for the door being configured. Press Enter. The screen displays:

20. DEVICE TAMPER REPORT (0-32) : 1?

32. Type a report number for the activation of the VIP tamper switch. After pressing Enter, the command prompt is displayed.

6.3.6 FORGIVE

The FORGIVE command resets the anti-passback status of all command keys in the system. It has the same effect on anti-passback status as disruption of power to the ACU. In either case, the Alto 818 resets the location of each key holder to UNKNOWN. Anti-passback status is then set to either IN or OUT the next time each key holder uses the command key.

The KEY command (see Section 6.3.10) can be used to reset anti-passback status for individual key holders.

6.3.7 GROUP

The GROUP command provides the quickest way to add command keys to the database or to modify the codes of a large number of keys. First, the group parameters are defined. Then all the keys having all these parameters in common are presented, one at a time, to a proximity sensors. The Alto 818 reads, prints (or displays), and stores in memory the code for each command card presented to the specified reader. Model 1030 and 1040 keys must have one of the facility codes (main or alternate) which have previously been defined with the SYSTEM command.

The name of command key holders may be entered later using the KEY command. The prompts for the GROUP command are shown in Figure 6-3.

```

2. ACCESS CODE (0-120): 0?
3. PRIVILEGED (Y/N): N?
4. TRACE (Y/N): N?
5. LOCATION (IN/OUT/UNKNOWN): UNKNOWN?
  SENSOR (1-8)?
  PRESENT KEYS TO SENSOR
  PRESS ANY KEY TO STOP
    
```

Figure 6-3: GROUP Command Prompts

1. At the command prompt, type GR and press Enter. The screen displays:

```
2. ACCESS CODE (0-120): 0?
```

2. Type the access code to be assigned to the command key group being added. Press Enter. The screen displays:

```
3. PRIVILEGED (Y/N): N?
```

3. Type Y or N as required and press Enter. The screen displays:

4. TRACE (Y/N) : N?

4. Type Y or N as required and press Enter. The screen displays:

5. LOCATION (IN/OUT/UNKNOWN) : UNKNOWN?

5. Type IN or OUT or accept the default, UNKNOWN. Press Enter. The screen displays:

SENSOR (1-8)?

6. Type the door number of the sensor to which the command keys will be presented. Press Enter. The screen displays:

**PRESENT KEYS TO SENSOR
PRESS ANY KEY TO STOP**

7. Present keys to the designated sensor one at a time. The terminal will display the key code of each card as it is read. When all command keys of the group have been entered into the Alto 818 database, press any key to stop. The command prompt is displayed.

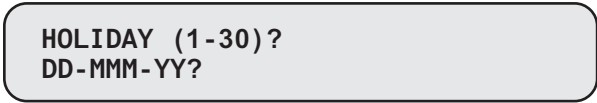
6.3.8 HELP

The HELP command displays a list of valid commands.

6.3.9 HOLIDAY

The Alto 818 can retain in memory the dates of up to 30 holidays which are specified by the HOLIDAY command. Since holidays are defined by day, month, and year, they must be updated annually in accordance with the yearly calendar. The HOLIDAY command prompts are shown in Figure 6-4. A HOLIDAY command setup sheet may be found in Appendix B.

The use of the HOLIDAY command interrelates with other commands that use time intervals if HOL is specified for a day when a specific time interval is applicable. When HOL is entered for any time interval in the system, all holidays specified with the HOLIDAY command will apply to that time interval.



**HOLIDAY (1-30)?
DD-MMM-YY?**

Figure 6-4: HOLIDAY Command Prompts

The holidays are entered as follows:

DD = Day of the month (01-31)
MMM = Month of the year (JAN, FEB, MAR, etc.)
YY = Year (95, 96, etc.)

For example, American Independence Day 1998 would be entered as 04 JUL 98.

The HOLIDAY command must be evoked for each holiday that is to be observed. To define holidays, proceed as follows:

1. From **YOUR COMMAND?** prompt, type **HOL** and press Enter. The screen displays:

HOLIDAY (1-30)?

2. Enter the number of the holiday to be defined and press Enter. The screen displays:

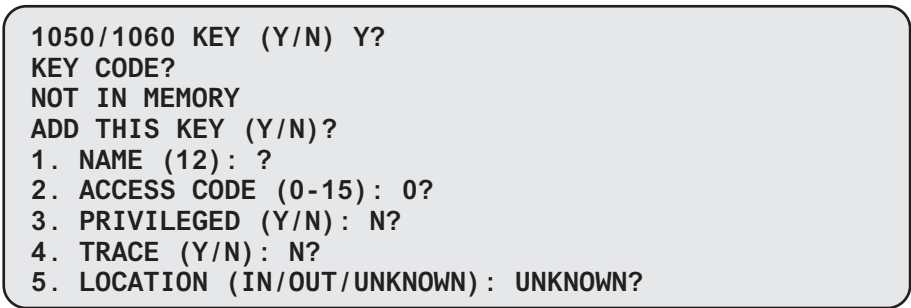
DD MMM YY?

4. Enter the date as described in Section 6.1; press Enter. The command prompt is displayed.

6.3.10 KEY

The KEY command is used to enter key holder codes and names. If key holder names are not required, keys can be grouped by their access codes and entered by use of the GROUP command (see Section 6.3.7).

The screen prompts for the KEY command are shown in Figure 6-5.



```
1050/1060 KEY (Y/N) Y?  
KEY CODE?  
NOT IN MEMORY  
ADD THIS KEY (Y/N)?  
1. NAME (12): ?  
2. ACCESS CODE (0-15): 0?  
3. PRIVILEGED (Y/N): N?  
4. TRACE (Y/N): N?  
5. LOCATION (IN/OUT/UNKNOWN): UNKNOWN?
```

Figure 6-5: KEY Command Prompts

1. At the command prompt, type K and press Enter. If 1050 or 1060 keys are being used along with either 1030 or 1040 keys, the next line will be displayed:

1050/1060 KEY (Y/N) Y?

2. If a 1050 or 1060 key is to be input type Y; for 1030 or 1040 keys type N. Type N for digital keys. Press Enter. The screen displays:

KEY CODE?

3. The key code can be found on one edge of the command key.

The 1050 keys may have code numbers from 1 to 24,040,016; and the 1060 keys may have code numbers from 24,040,017 to 99,999,999.

If VIP ONLY key codes are to be entered, refer to the SYSTEM command field 16 for the number of digits, 4–8. The number of digits entered for KEY CODE must be the same as the VIP ONLY value.

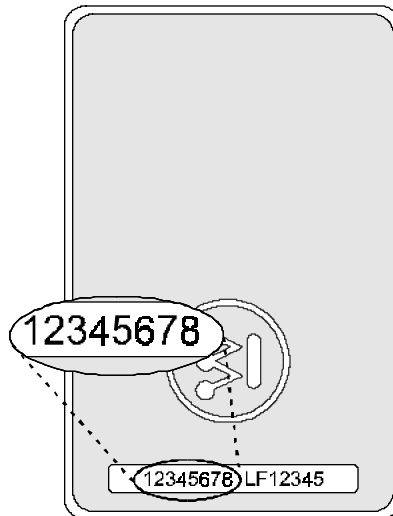


Figure 6-6: Command Key Code Number

Type the code number and press Enter. If the key code is currently in the database, prompt 1 is displayed. If the key code has not been previously entered into the database, the screen displays.

**NOT IN MEMORY
ADD THIS KEY (Y/N)?**

5. If N is entered, the command prompt line is displayed. If Y is entered the screen displays:

1. NAME (12): ?

6. A unique name with a maximum of 12 characters and spaces is entered in this field for each key holder if keys are to be defined by both names and codes. Names greater than 12

characters will be truncated. Similar key holder names may need to be modified to assure that they are unique. Two John Browns might be differentiated by middle initial: John J Brown and John B Brown. Logs for key holder activity will identify the key by both the code and the name specified in this field. Type the name and press Enter. The screen displays:

2. ACCESS CODE (0-15) : 0?

7. Type the appropriate code for the card holder.

Access code 0 might be entered for a card holder who reports a lost key or is taking a leave of absence. If an attempt is made to gain access with a command key with a 0 code, an access denied log will be generated.

Press Enter. The screen displays:

3. PRIVILEGED (Y/N) : N?

8. Enter Y only if the system is set up to use building modes and the card holder will be changing building modes from a remote station. In all other cases, the default N is appropriate. Select Y or N and press Enter. The screen displays:

4. TRACE (Y/N) : N?

9. Type Y and press Enter if a key trace report will be generated for the card holder. The key trace function is only valid where it is enabled with the DOOR command. For no key trace report, press Enter to accept the default, N. The screen displays:

5. LOCATION (IN/OUT/UNKNOWN) : UNKNOWN?

10. This field is applicable only when anti-passback has been enabled. The default, UNKNOWN, may be accepted for all users. When anti-passback is in place, the Alto 818 will change the key holder's location appropriately the next time they access a controlled door. If required, IN or OUT may be entered. Make a location selection and press Enter. The command prompt is displayed.

To display the PIN for a key generated by the system, use the PRINT KEY command entering Y to the PRINT PINS prompt. The screen prompts for PRINT KEY, followed by the resulting output, are shown in Figure 6-7.

```

PRINT IN ALPHABETICAL ORDER (Y/N): ? Y
ANY QUALIFIERS (Y/N): ? Y
1A. 1060 KEY TYPE (Y/N): ? Y
1B. 1050 KEY TYPE (Y/N): ? Y
1C. 1040/1030 KEY TYPE (Y/N): ?
2. ACCESS CODE (0-120): ? 1
3. PRIVILEGED (Y/N): ?
4. TRACE (Y/N): ?
5. LOCATION (IN/OUT/UNKNOWN): ?
PRINT PINS (Y/N): ? Y

```

```

P=PRIVILEGED T= TRACE I=IN O=OUT H=HOST

```

```

9896 12345678 1 PT FRANKIN JOS
3419 87654321 1 T NEWBERG ALIC
2252 246813579 1 P O WELCH MIKE

```

Figure 6-7: PRINT KEY Screen with Resulting Output

6.3.11 LIMIT

This command is applicable only if the Alto 818 system is set up to use building modes, and open, closed, and station sensors have been defined with the DOOR command (see Section 6.3.5). Entering the LIMIT command places the building in the building-limited mode.

6.3.12 MODEM

An SE 5200 Smart Modem can be used to interface the ACU with a remote terminal via the host port on the Alto 818. When a modem is used for this purpose, the modem command is used to: (1) set the building ID messages that the Alto 818 will use for identification during communications with the remote terminal, (2) assign the phone numbers of the remote terminal modem, (3) define the number of times the Alto 818 should attempt to place a call with the remote terminal modem, and (4) enable or disable the CALL BACK function. All MODEM command prompts are shown in Figure 6-8.

1. At the YOUR COMMAND? prompt, type MOD and press Enter. The screen displays:

```

1. BLDG ID (72):
?

```

This field is used to set up the building ID messages that the Alto 818 will use for identification purposes when communicating with a remote terminal by means of a smart modem. Three messages are possible. Each ID message must be no longer than 72 characters (including spaces). Enter messages and press Enter. The screen displays:

2. TELEPHONE (24) :
?

2. This field is used to set up the host phone numbers. Phone numbers of no more than 24 numbers (including spaces) are possible. Two additional lines allow a total of three phone numbers to be entered. The system will make attempts to call the host, trying the given numbers sequentially. If only one remote location is to be dialed, enter its number three times. Make the desired entries and press Enter. The screen displays:

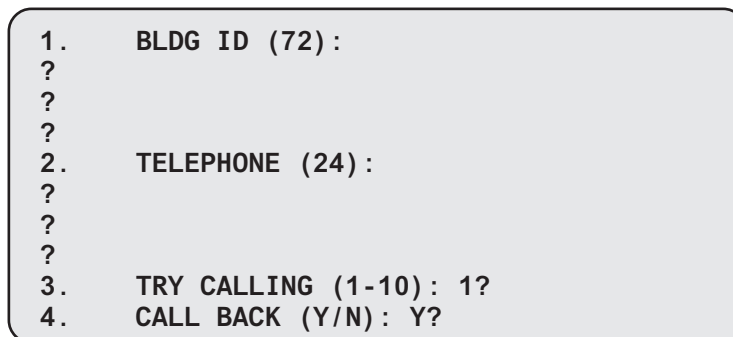
3. TRY CALLING (1-10) : 1?

3. Type the number of times, from 1 to 10, that the Alto 818 should attempt to dial the three numbers entered in field 2 and press Enter. The screen displays:

4. CALL BACK (Y/N) : Y?

4. The CALL BACK function is used to protect the system from break-ins via the telephone lines. If the CALL BACK function is enabled, when anyone dials the Alto 818 telephone number, the ACU will not maintain the connection. Instead, it will hang up and then dial out to the numbers entered in field 2. Thus anyone attempting to access the system via the phone lines from any source except the intended remote location will be disconnected. And, since the remote location phone numbers exist only as listed numbers in the ACU database, these numbers are not available to anyone except rank A system operators through the use of the PRINT MODEM command.

The default is Y; type N to disable the call-back feature. Press Enter. The command prompt is displayed.

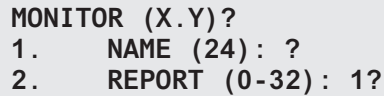


```
1. BLDG ID (72) :  
?  
?  
?  
2. TELEPHONE (24) :  
?  
?  
?  
3. TRY CALLING (1-10) : 1?  
4. CALL BACK (Y/N) : Y?
```

Figure 6-8: MODEM Command Prompts

6.3.13 MONITOR

The MONITOR command is used to link activity at one or more of the system monitor points to a specific report. These monitor points are the sets of contacts, four sets per unit, on an MSM. The prompts for the MONITOR command are shown in Figure 6-9. A MONITOR command setup sheet may be found in Appendix B.



```
MONITOR (X.Y)?  
1. NAME (24): ?  
2. REPORT (0-32): 1?
```

Figure 6-9: MONITOR Command Prompts

Generally, this command should not be used to generate a report for door switch and REX monitoring points since these points are linked to reports through the DOOR command. Use this command to set the report for the door switch and REX to 0, no report.

1. Type MON at the command prompt. The screen displays:

MONITOR (X.Y)?

2. Enter the designation for the monitor point to be configured. X is the sensor port number to which the MSM is connected. Y is the contact number on the specified MSM, 1 through 4. Press Enter. The screen displays:

1. NAME (24): ?

3. The name given to a monitor point should be descriptive. To facilitate later modifications to the Alto 818 configuration and database, unused points should be named accordingly. Type a name, a maximum of 24 characters in length including spaces. Press Enter. The screen displays:

2. REPORT (0-32): 1?

4. Select the report number, default 1, to respond to log events. Press Enter. The command prompt is displayed.

6.3.14 OPEN

This command is applicable only if the Alto 818 system is set up to use building modes and open, closed, and station sensors have been defined with the DOOR command (see Section 6.3.5). Entering the OPEN command places the building in the building-open mode.

6.3.15 RELOCK

The RELOCK command reverses the UNLOCK command. This command applies only after the UNLOCK command has been invoked. It relocks doors that were unlocked by the UNLOCK command, and returns the door access status to its preconfigured parameters as set up in the database.

```
YOUR COMMAND?  RELOCK
DOOR (1-8 OR 0 FOR ALL)?
```

6.3.16 REPORT

The report command is evoked for each report that is to be assigned (up to 32 reports). Report 1 comes from the factory preprogrammed for a report which will be sent to the host at all times, all days, including holidays. If you wish to keep the default settings for report 1, proceed to report 2, referring to the completed REPORT command database setup sheets for the parameters to be entered for each report being defined. The default menu for the REPORT command is shown in Figure 6-10.

To enter the reports in the database, proceed as follows:

1. From the command prompt, type REP and press Enter. The screen displays:

```
REPORT (1-32)?
```

2. Type the number of the report to be defined and press Enter. The screen displays:

```
GO TO (1-5)?
```

```

GO TO (1-5)?
1. SEND TO HOST
  OPEN (Y/N) N?
  LIMITED (Y/N) N?
  CLOSED (Y/N) N?
  00:00-00:00?
  00:00-00:00?
  00:00-00:00?
2. CLOSE LATCHED CONTACT
  OPEN (Y/N) N?
  LIMITED (Y/N) N?
  CLOSED (Y/N) N?
  00:00-00:00?
  00:00-00:00?
  00:00-00:00?
3. CLOSE CONTACT (0-16)?
  OPEN (Y/N) N?
  LIMITED (Y/N) N?
  CLOSED (Y/N) N?
  00:00-24:00 SUN MON TUE WED THU FRI SAT HOL?
  00:00-00:00?
  00:00-00:00?
4. PREVENT BUILDING CLOSURE (Y/N) N?
5. PRINT * (Y/N) N?

```

Figure 6-10: REPORT Command Prompts

3. Press Enter to begin with the first field. Type a number in the range and press Enter to skip to another field. The field 1 display is:

```

1. SEND TO HOST
  OPEN (Y/N) N?

```

4. Type Y to send the report to the host or make no entry to accept the default, or current entry, and press Enter. The screen displays:

```

LIMITED (Y/N): N ?

```

5. Repeat instructions for step 3, entering the Y or N to send the report to the host when the building is in LIMITED mode. Repeat again for the next displayed line for CLOSED mode. The screen displays:

```

00:00-00:00?

```

6. Up to three time intervals during which the report should be sent to the host may be defined. Time intervals are in addition to modes selected above. Type the required time interval and effective days and press Enter. The screen displays:

```

2. SEND TO TERMINAL AND CLOSE LATCHED CONTACT
  OPEN (Y/N) N ?

```

7. Repeat steps 4 through 6 to specify the conditions under which to close the alarm contact when the report is generated. The screen displays:

3. SEND TO TERMINAL AND CLOSE CONTACT (0-16) : 0?

8. If you wish a relay to close when this report is generated, type in the relay number, 1 to 16, and press ENTER. The default, 0, will not close a contact. The screen now displays the queries for building modes and time intervals. Follow the instructions in steps 4 through 6 above. The screen displays:

4. PREVENT BUILDING CLOSURE (Y/N) N ?

9. If you wish the reported condition to prevent building closure type Y and press ENTER. The screen displays:

5. PRINT * (Y/N) N ?

10. If Y is selected for this field, an asterisk (*) will precede the report message thus acting as a flag to the operator that a condition exists which requires attention. In addition, if a modem is installed, the asterisk will cause the remote location to be dialed immediately and the report transmitted. Type Y or N and press Enter. This command prompt is displayed.

6.3.17 RESET

The RESET command is the software equivalent to pressing the reset switch on the ACU PCA. All operator override commands are disabled and the system returns to the operation mode.

6.3.18 SHUNT

The SHUNT command is used to turn off a specific access control or alarm monitoring function while the rest of the system is under normal operation. All activities associated with the shunted devices are temporarily disabled. When the SHUNT command is entered, the Alto 818 displays the categories of functions that may be shunted, as follows:

**YOUR COMMAND? SHUNT
(DOOR/MONITOR/COAX/SENSOR/MSM/TAMPER/POWER/VIP/VIPTAMPER/READER/READERTAMPER) ?**

After the list is displayed, enter the type of function that you wish to shunt. If DOOR, MONITOR, COAX, SENSOR, MSM, or VIP is selected, enter the number of the door, monitor point, etc., to be shunted.

The SHUNT command disables the following log event reports:

- COAX FAILURE
- DEVICE TAMPER
- DOOR FORCED OPEN
- DOOR OPEN TOO LONG
- MONITOR POINT ACTIVE
- MSM FAIL
- SENSOR FAIL
- SENSOR FAIL
- COAX FAIL
- SNET READER FAIL
- TAMPER
- VIP FAIL
- VIP TAMPER

SHUNT COMMAND EXAMPLES

Assume it is necessary to hold open a controlled door because office furniture is being moved in. A guard could be posted at the door to prevent unauthorized entries, and the door could be shunted to prevent a DOOR HELD OPEN TOO LONG report from being generated. Or, assume that an unauthorized entry has been made, causing a DOOR FORCED OPEN report to be generated. In this case, the damage to the door must be repaired before the door can be returned to normal operation.

In both the cases, the operator would invoke the SHUNT command, enter the DOOR function to be shunted, and then enter the number of the door. This action prevents the generation of door reports from that door until the UNSHUNT command (see Section 6.3.24) is used to reverse the action of the SHUNT command.

6.3.19 SILENCE

The SILENCE command is for systems using the set of latched contacts (L-ALARM) on the SE 778-A Annunciator/Control module (Ann/C). The latched contacts are programmed in the system database to close for specific alarm conditions during specific time intervals. Once closed, this set of contacts can be opened (unlatched) only by operator intervention using the SILENCE command.

6.3.20 STATUS

When the STATUS command is invoked, a system status report is generated and displayed at the terminal port (the report can be printed, if required). Status is reported on the building mode (open, limited, or closed), tamper switches, system power, system sensors, MSMs, VIPs, and VIP tamper switches.

The anti-tamper monitoring function monitors the status of the tamper switch under the cover of the Alto 818 and, if used, of an auxiliary tamper input from the RS-485 connector (usually a tamper switch located under the cover to the equipment enclosure in which the ACU is housed).

Building Mode Tamper Power Alarm										
-----0----- ----A--- ----- -----										
#####	Door	Coax	SnSr	Reader	VIP	MSM	MP1	MP2	MP3	MP4
--#1--	-----	-----	-----	-----	---NP---	---F-	-----	-----	-----	-----
--#2--	-----	-----	-----	-----	---NP---	---F-	-----	-----	-----	-----
--#3--	-----	-----	-----	-----	---NP---	---F-	-----	-----	-----	-----
--#4--	-----	-----	-----	-----	---NP---	---F-	-----	-----	-----	-----
--#5--	-----	-----	-----	-----	---NP---	---F-	-----	-----	-----	-----
--#6--	-----	-----	-----	-----	---NP---	---F-	-----	-----	-----	-----
--#7--	-----	-----	-----	-----	---NP---	---F-	-----	-----	-----	-----
--#8--	-----	-----	-----	-----	---NP---	---F-	-----	-----	-----	-----
O = Open L = Limited C = Closed F = Fail S = Shunted A = Active U = Normal Unlock NE = Not Enabled H0 = Held Open F0 = Forced Open TS = Tamper Shunted TA = Tamper Active										

Figure 6-11: Example of STATUS Display

The power failure monitoring function is operative only when the Alto 818 is powered by an uninterruptible power supply using DC battery backup power. On such systems, the POWER FAIL message indicates that the system is operating on DC battery power and that the battery power is getting low. Power status is determined by monitoring pin 7 on the power connector of the Alto 818. On systems that do not use backup battery power, the power failure report (field 5) in the SYSTEM command should be set to 0.

System faults that are reported include coaxial cable failure, sensor failure, MSM failure, power failure, and tamper detection. Once the latched alarm contact (L-ALARM) on the Ann/C is activated, the word ALARM is printed in status reports until the SILENCE command is entered.

The Alto 818 automatically sends a status report to the terminal port when entering or attempting to enter the building-closed mode from a station sensor. The status report lists all active events even though the actual reporting time may not be valid. An example of a status display is shown in Figure 6-11.

6.3.21 SYSTEM

The SYSTEM command is used to define parameters that affect the overall operation of the Alto 818 system. These include specifying the type of command keys to be used, configuring the ACU for terminal and/or host communications and assigning reports to a number of system activities. The complete list of SYSTEM command prompts is shown in Figure 6-12.

1. At the YOUR COMMAND? prompt, type SY and press ENTER. The screen displays:

GO TO (1-22)?

2. Type a prompt number and press ENTER. If 1, the default, is selected, the screen displays:

1. 1060 KEY TYPE (Y/N): Y?

3. Fields 1 through 3 are used to specify the command key types used in the system. Each system can accommodate more than one type of key. However, if 1030 keys are used, 1040 keys cannot be used, and vice versa. Type Y or N and press Enter. The screen displays:

2. 1050 KEY TYPE (Y/N): N?

4. Type Y or N and press Enter. The screen displays:

3. 1040/1030 KEY TYPE (0/1040/1030): 1040?

5. Enter the key type to be used and press Enter. If 1030 or 1040 is entered in field 3, the system will go to fields 3A and 3B. If 0 is entered, these field will be skipped. The screen displays:

3A. FACILITY CODE: A000?

6. This field applies to 1030 and 1040 command keys only. The facility code, consisting of a letter and three numerical digits, is the second set of characters printed on these keys. Type the required code and press Enter. The screen displays:

3B. ALTERNATE FACILITY CODE: A000?

7. If a second set of command keys is to be used, the facility code for these keys may be entered here. After typing the desired code or leaving the default, press Enter. The screen displays:

4. TAMPER REPORT (0-32): 1?

8. The tamper report covers tamper activity detected by the tamper switch on the ACU cover and other devices which do not generate a unique log event. The field default is 1; 0 indicates no tamper report. Type the desired report number and press ENTER. The field displays:

5. POWER FAIL REPORT (0-32): 1?

9. A power fail report can be generated when the Alto 818 is powered by an SE 3708C Uninterruptible Power module. The report will occur if the AC power has failed and the backup battery charge is getting low. The field default is 1; 0 indicates no power fail report. Type the desired report number and press ENTER. The field displays:

**6. BLDG SHOULD BE CLOSED:
00:00-00:00 ?**

10. When building modes are to be used, field 6 is used to specify up to four time intervals during which the building should be in the closed mode. At these times, a building open reminder report (as specified in field 7) is generated if the building is in any mode other than closed. If no time intervals are specified, this function is disabled. Enter the first time interval and press Enter.

CAUTION:

These time intervals do not close the building. The building mode may be changed to closed from the terminal, host or from an L/C station.

Enter up to three additional time intervals as required. The screen displays:

7. BLDG SHOULD BE CLOSED REMINDER (0-240) : 0?

11. If the building mode is not closed during the time periods specified in field 6 (if any are specified), a reminder can be displayed on the terminal or sent to a host. The reminder will be repeated at intervals from 1 to 240 minutes as specified by field 7. If no time intervals are specified in field 6, this field should be left with the 0 default setting. Type the desired number and press Enter. The screen displays:

8. HOST BAUD: 9600?

12. This field is used to set the baud rate for communication between the Alto 818 and a host system. The rate may be 300, 1200, 2400, 4800, or 9600; the default is 9600. Enter the rate required by the modem and host configuration and press Enter. The screen displays:

9. TERMINAL BAUD: 300?

13. Like the host, the terminal to ACU communication may be set at baud rates 300, 1200, 2400, 4800, or 9600 as defined by the terminal configuration. The default for the ACU and the SE 57101 terminal is 300.

Because the baud rate of the Alto 818 and the terminal must be identical, use the following procedure to make a change.

- a. From the terminal, use the SYSTEM command to set the ACU baud rate.

```

GO TO (1-22)?
1. 1060 KEY TYPE (Y/N): Y?
2. 1050 KEY TYPE (Y/N): N?
3. 1040/1030 KEY TYPE (0/1040/1030): 1040?
3A. FACILITY CODE: A000?
3B. ALTERNATE FACILITY CODE: A000?
4. TAMPER REPORT (0-32): 1?
5. POWER FAIL REPORT (0-32): 1?
6. BLDG SHOULD BE CLOSED:
   00:00-00:00 ?
   00:00-00:00 ?
   00:00-00:00 ?
   00:00-00:00 ?
7. BLDG SHOULD BE CLOSED REMINDER (0-240): 0?
8. HOST BAUD: 9600?
9. TERMINAL BAUD: 300?
10. OPERATOR OVERRIDE REPORT (0-32): 1?
11. ADDRESS (0-240): N?
12. HOST XON/XOFF (Y/N): N?
13. TERMINAL XON/XOFF (Y/N) N?
14. AUTO FORGIVE TIMES AND DAYS:
   00:00-00:00 ?
   00:00-00:00 ?
   00:00-00:00 ?
   00:00-00:00 ?
15. READER DISABLE TIME (0-240): 10?
16. VIP ONLY KEY DIGITS (4-8): 4?
17. PIN DIGITS (4-5): 4?
18. PIN SEED 0000?
19. PIN GRACE PERIOD (10-240): 10?
20. PIN RETRY (0-5): 0?
21. DURESS ENABLE (Y/N): Y
21A. DURESS REPORT (0-32): 1?
22. SHOW KEY NUMBER FOR "VIP ONLY\ KEY" (Y/N): N?

```

Figure 6-12: SYSTEM Command Prompts

b. Reset the ACU by pressing the reset button on the Alto 818 PCA or by typing the command RESET from the terminal. The new baud rate will also become effective if the power to the ACU is cycled off and then on.

c. Change the terminal baud rate to be compatible with the rate set for the ACU.

d. Communication between the Alto 818 and the terminal is restored, at the new baud rate.

If communication between the terminal and the ACU is lost due to incompatible baud rates, use the following procedure:

a. Reset the ACU by pressing the reset button on the Alto 818 PCA while holding down the goof switch. This will restore the default value of 300.

- b. Set the terminal baud rate to 300. Communication between the Alto 818 and the terminal should be restored.
- c. Use the procedure above to change the baud rate.

The screen displays:

10. OPERATOR OVERRIDE REPORT (0-32) : 1?

- 14. An operator override condition occurs each time an operator enters a direct command (CLOSE, LIMIT, OPEN, RELOCK, SHUNT, SILENCE, UNLOCK, and UNSHUNT). To generate a report for an operator override, type the desired report number (0 for no report) and press ENTER. The screen displays:

11. ADDRESS (0-240) : 0?

- 15. If the Alto 818 is operating in the E-mode, reporting to a host system, the address of the ACU must be set to a number between 1 and 240. The address must be identical with the address assigned by the host system to this Alto 818. If the Alto 818 is being used in the S-mode, terminal communication only, the default value of 0 may be used. Type the desired address and press ENTER. The screen displays:

12. HOST XON/XOFF (Y/N) : N?

- 16. The XON/XOFF parameter of host to Alto 818 communications can be set to Y to allow control of scrolling data logs. When enabled, the keyboard input CTRL-S will stop scrolling data; CTRL-Q will allow the scroll to continue: Data displayed is paused. The default for XON/XOFF is N which disables the function. Type Y or N and press ENTER. The screen displays:

13. TERMINAL XON/XOFF (Y/N) N?

- 17. Read the description for prompt 12 above. Select Y or N for terminal XON/XOFF and press enter. The screen displays:

**14. AUTO FORGIVE TIMES AND DAYS:
00:00-00:00 ?**

- 18. The AUTO FORGIVE TIMES parameters are functional only when anti-passback control is used. At the times entered for field 14, the location of all command key holders is set to UNKNOWN and no anti-passback violations are generated. Type the desired times and days and press Enter. The three following prompts allow additional intervals to be entered. The screen displays:

15. READER DISABLE TIME (0-240) : 10?

19. This field is used to select a period of time between 1 and 240 seconds during which a reader cannot read another command key if access has been denied to a user. The default time is 10 seconds. If 0 is entered, the function is disabled. Press Enter after making a selection. The screen displays:

16. VIP ONLY KEY DIGITS (4-8) : 4?

20. This field is used if a VIP2 is the only reader device used on one or more doors. The number of digits entered here must be the same as the number used for entering key codes. Select a number from 4 to 8 and press Enter. The screen displays:

17. PIN DIGITS (4-5) : 4?

21. A 4 or 5 is entered in this field, depending of the number of digits to be used for personal identification numbers (PINs). The PIN is the used gain access at a VIP2 reader. The default, 4, may be left if no keypads will be used. The number of PIN digits must be less than or equal to the number entered for prompt 16. VIP ONLY KEY DIGITS. Type 4 or 5 and press enter. The screen displays:

18. PIN SEED 0000?

22. Field 18 is used if a VIP2 is to be used along with a proximity reader at one or more doors. In such configurations, the system will use this PIN seed in conjunction with the command key code to generate PINs. After the PIN seed number is entered, the PRINT KEY command can be used to list the PIN for each key holder.

The PIN seed must have the same number of number of digits as the PIN digits defined in field 17. If 4 PIN digits is selected and a 5-digit seed is entered, the seed is truncated to 4 digits. If 5 PIN digits is selected and a 4-digit seed is entered, a leading 0 is added to the seed.

A 4-digit PIN seed may be any number between 0000 and 9999, 0000 default. A 5-digit PIN seed may be any number between 00000 and 99999, default 00000. If the PIN seed is changed, all PIN codes are automatically changed. This feature can be useful if security has been compromised by unauthorized individuals obtaining PINs.

After entering the PIN seed, the screen displays:

19. PIN GRACE PERIOD (10-240) : 10?

23. The PIN grace period specifies the amount of time allowed to complete the PIN entry and, present a command key if a proximity reader is also used. The PIN may be entered before or after the command key is presented. The default for this setting is 10 seconds. Type a value and press Enter. The screen displays:

20. PIN RETRY (0-5) : 0?

24. Field 20 is used to specify the number of retries, from 0 to 5, that can be made to enter a PIN before an ACCESS DENIED PIN CODE log message will be generated. The default setting is 0, no retries. A user may press the # or * key to restart PIN entry when an error has been made.

21. DURESS ENABLE (Y/N) : Y

25. A duress code is a variation of a user's normal PIN. When entered, it can be used to signal a security officer or other person of a problem at an entrance. This can be an added safety factor when users are entering or exiting during late-night hours. The default is N. Type Y to enable the duress code function and press Enter. The screen displays.

21A. DURESS REPORT (0-32) : 1?

26. This field is used to assign a report number, 1 to 32, if the duress function was enabled above. If no report is to be generated, enter 0 here.

The report generated for a duress situation can be very important. It can provide the key code of the individual who has entered the duress code and can be used to trigger silent devices, generate dial-up modem messages, turn on a closed circuit TV camera or other security action.

Type in the desired report number and press Enter. The screen displays:

22. SHOW KEY NUMBER FOR "VIP ONLY\ KEY" (Y/N) : N?

27. The parameter set with this prompt is valid access is controlled by a VIP2 without the addition of a proximity reader. The default is N which means that when activity for the VIPs is to be logged, the PIN will not be displayed or printed. This may be desirable for security reasons. Type Y or N as required and press Enter. The command prompt is displayed.

6.3.22 TIME

The TIME command is used during database setup to set the real-time clock to indicate current date and time. This command is used thereafter to make any changes to the time and/or the date that are required. Notably, Alto 818 systems that operate in the USA must have the time changed twice a year to make allowances for daylight savings time. Since the time interval time settings and all system activity data log entry times are based on the TIME command settings, these settings must be accurate.

After entering TI at the command prompt, the time is displayed in the format:

DAY DD-MM-YY HH-MM

DAY = SUN, MON, TUE, WED, THU, FRI, SAT

DD = Day of the month (01-31)
MMM = Month of the year (JAN, FEB, MAR, etc.)
YY = Year (95, 96, etc.)
HH = Hours of the day in 24-hour time (00-23)
MM = Minutes in the hour (00-59)

To change to the current time and date, first enter the day of the week (MON, TUE, WED, THU, FRI, SAT, or SUN, as appropriate), followed by the current day of the month (01-31), followed by the current month (JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, or DEC, as appropriate), followed by the last two numbers in the current year. Then set the time by entering the hour (00-23) and then the minute (0-59).

For example, to set the time and date as Friday, June 16, 1995, 1:30 PM, type **FRI <space> 16–JUN–95 <space> 13:30** and press enter key:

Screen displays:

FRI 16-JUN-95 13:30

To verify the time and date settings repeat the TIME command or type PRINT TIME at the command prompt and press Enter.

6.3.23 UNLOCK

The UNLOCK command is used to unlock any system door. Once a door is unlocked, it remains unlocked until the RELOCK command is entered, or system power is lost, or the building mode changes.

When the UNLOCK command is entered, the display is as follows:

YOUR COMMAND? UNLOCK
DOOR (1-8 OR 0 FOR ALL)?

Type the number of the door to be unlocked or select 0 for all doors. Press Enter and the command prompt is displayed.

6.3.24 UNSHUNT

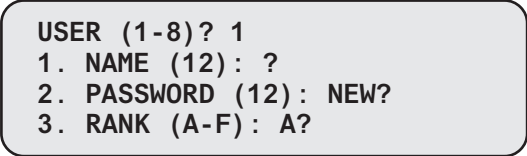
The UNSHUNT command is used to reverse the SHUNT command. The screen for the UNSHUNT command is as follows:

```
YOUR COMMAND? UNSHUNT
(DOOR/MONITOR/COAX/SENSOR/MSM/TAMPER/POWER) /VIP/VIPTAMPER/READER/READERTAMPER)?
DOOR 1-8)?
```

6.3.25 USER

Throughout this manual, the word operator has been used to describe individuals who have access to the system terminal in order to use the operate and program commands. However, in the program commands, the word user is applied to individuals who have access to the system commands, i.e., the operators and the system administrator.

This command is used to enter the name, password and rank of up to eight users. Because the Alto 818 recognizes a user by the password entered, each password must be unique. Users should know only their own password; the list of passwords for all users should be known only to the system administrator and should be kept under lock and key. The user rank controls which commands the user may execute; rank A has access to all commands. The prompts for this command are shown in Figure 6-13. A USER setup sheet is included in Appendix B.



```
USER (1-8)? 1
1. NAME (12): ?
2. PASSWORD (12): NEW?
3. RANK (A-F): A?
```

Figure 6-13: USER Command Prompts

To define the system users, proceed as follows:

1. From the **YOUR COMMAND?** prompt, type **US** and press Enter. The screen displays:

```
USER (1-8)? 1
```

Accept the default 1 or type another user number, 2–8, and press Enter. The screen displays:

```
1. NAME (12) ?
```

2. Type a user name, up to 12 characters in length. Press Enter. The screen displays:

2. PASSWORD (12) : NEW?

3. Type the password, up to 12 characters in length. Press Enter. The screen displays:

3. RANK (A-F) : A?

4. Type the rank for the user and press Enter. The command prompt is displayed.

6.3.26 VERSION

This command displays the firmware version of the Alto 818 in the format:

(C) 1994 - Westinghouse Security Electronics - 62109112001C 9C47

Please have this information available before seeking technical support from your dealer, installer or WSE Customer Service.

6.3.27 XLOAD

The XLOAD command is used to load the system database into the Alto 818's memory from a disk or diskette file created with the XSAVE command (Section 6.3.28). To load a database into ACU memory from a backup diskette, proceed as follows:

1. Follow steps 1 and 2 in the XSAVE procedure. If the database was backed up to a diskette, insert the diskette in the appropriate drive.
2. When the screen displays YOUR COMMAND?, type XLOAD and press ENTER.
3. On the PC, press Alt-M to access the menu. Select SEND A FILE and press ENTER.
4. Type the name of the source file and press ENTER.
5. Select XMODEM CHECKSUM and press ENTER.

The ACU will begin to receive data from the PC. Reset the ACU when the data transfer is complete.

6.3.28 XSAVE

The XSAVE command is used to save the system setup data to a hard drive or diskette. The file transfer is via an Xmodem program executed with an IBM PC or equivalent. There are several Xmodem file transfer programs that can be used for this purpose. Crosstalk and TERMINAL.EXE are two examples.

In case of a power failure to the ACU, the Alto 818's internal battery will provide power to the system memory for as long as one year. However, should any emergency event occur that causes the database to be tampered with or deleted from memory, a backup to a hard disk or a diskette containing the system database setup will prove invaluable. Also, in the event that the ACU requires replacement, the time-consuming process of setting up the database for the new unit can be eliminated if the database from the old unit has been saved.

To download the ACU database to the PC using TERMINAL.EXE, proceed as follows:

1. Connect the ACU host port to the desired communication port of the PC using a null modem cable.
2. Start the terminal program on the PC setting the parameters as follows:

Baud	set to same rate as the ACU
Data Bits	7
Parity	ODD
Com Port	set as required

3. On the PC, press Alt-M to access the menu. Select RECEIVE A FILE and press ENTER.
4. Select XMODEM CHECKSUM and press ENTER.
5. Type the name of the destination directory and file, including extension, and press ENTER.

The PC will begin to receive data from the ACU. Reset the ACU when the data transfer is complete.

SECTION 7: DATABASE SETUP

This section describes the procedures for setting up the database in the Alto 818. Refer to Section 6 for command descriptions.

7.1 OVERVIEW

Before the database can be set up, all database parameters should be determined and recorded in the setup sheets in Appendix B. All controlled doors, readers, monitor points, and relay outputs, etc. must be identified and defined. All log events will have to be identified and assigned a report number. Each individual who will be responsible for operating the system must have a password and user rank assigned. Finally, all card holder groups and individual card holders must be identified.

Database setup can be done before the Alto 818 is brought to the installation site and connected to the rest of the system components. However, the Alto 818 must be connected to a terminal and a power module. In addition, if command cards are to be set up with the GROUP command, a reader must be connected.

7.1.1 SYSTEM ADMINISTRATOR

The term 'system administrator' refers to the individual who has overall responsibility for the integrity of system security. The system administrator assigns user passwords and ranks through the USER command and should be the only person who knows these assignments.

The system administrator is responsible for database maintenance and should be the only person who has access to the XSAVE and XLOAD commands for database backup and restore purposes. Further, the system administrator is the only individual who can run diagnostics. These operations are all functions of authorization rank A.

7.1.2 USER AUTHORIZATION RANK

As used in this text, the terms operator and user are synonymous. System operators are those individuals who perform system functions by entering commands and data via the system terminal or host computer. The extent to which any given operator is permitted to control the system by the use of the Alto 818 commands is governed by that operator's user authorization rank.

During database setup, the USER command is used to assign up to 8 passwords and 6 user authorization ranks, rank A through F, for system users. Consequently, after the database is set up and the system is placed in operation, the availability of any system command to any operator

depends on the rank that they have been assigned. Refer to Table 6-2 for a user authorization rank matrix.

7.1.3 DEFAULT DATABASE PARAMETERS

All Alto 818 systems have been preprogrammed at the factory with default database parameters. The default parameters appear just to the left of the question mark at the end of most of the command prompts. Configuration data entered during initial system database setup will appear in place of the default parameters the next time the command is invoked.

A default password has also been assigned, a default access code has been set up for access code 1, and a default report has been set up for report 1.

DEFAULT PASSWORD NEW

To access the program commands for database setup purposes, each system comes with the default password NEW preassigned for user 1 with rank A. This is the password assignment that should be reserved for the system administrator. When the system administrator assigns a unique password for user 1, the password NEW is overwritten and will no longer be valid.

The user 1 password can be restored to NEW with a rank A by the following procedure:

1. Press and hold the goof switch down (Figure 2-3).
2. Press the reset switch.
3. After the reset is complete, release the goof switch.

DEFAULT ACCESS CODE 1

Unless modified during database setup operations, access code 1 provides access to all system doors at any time on all days of the week, including holidays. Since such an access code is often required for a limited number of personnel, it is recommended that the default values for access code 1 be retained and assigned during database setup to only to appropriate card holders.

DEFAULT REPORT 1

Unless modified during database setup operation, report 1 will be generated 24 hours a day, seven days a week, including holidays, for any log event(s) to which it is assigned. This default report 1, however, will record only the log events assigned to it and display them on the system terminal. No system action will occur such as sending the report to the host port, closing any set of relay contacts, preventing building closure, or printing an asterisk before the log entry.

Some log events, such as ACCESS GRANTED, EXIT GRANTED, OPERATOR OVERRIDE, do not usually require any system action and are logged mainly for record keeping purposes. The default report 1 can be assigned to all such log events.

7.2 PREPARATION FOR SETUP

A considerable amount of data must be gathered before a system database can be set up. During the database setup process, the system requests a number of data inputs. These inputs must be predetermined since they involve detailed information concerning both the system hardware and the owner's access control requirements.

The material in this section and the database setup sheets in Appendix B should be studied in advance of database setup to understand the parameters that need to be predetermined. A meeting with the owner is essential. The access codes and the reports must be carefully defined before the database setup process is attempted. The database setup sheets should be completely filled out.

7.2.1 TALK TO THE OWNER

A meeting with the owner must be held to review all system access control requirements as they pertain to the information required to set up the database. It is essential to obtain a precise definition of exactly what the owners need to protect with their system and how it can best be accomplished. Go over the database setup sheets to determine just what data needs to be provided. Take a copy of the installation plan to the meeting with the owner.

7.2.2 COMMAND KEYS

While the Alto 818 can read WSE 1030, 1040, 1050 and 1060 command keys, 1030 keys cannot be mixed with 1040 keys. Either 1030 or 1040 keys may be mixed with 1050 and 1060 keys. For facility code compatibility for any given set of keys, consult with WSE Customer Service Engineering.

7.2.3 LISTING CARD HOLDERS

A list that includes the name of every individual who will be issued a command card or be using a keypad must be compiled. This list must itemize the days of the week and the time intervals that each card holder or keypad user is authorized to gain entrance to each door in the system. Fill out the card holder setup sheets in Appendix B, noting if the assignment is for a VIP2-only user.

The names of the card holders/keypad users must be provided by the owner. Then, during the meeting with the owner, the precise access requirements of each card holder/keypad user must be determined and recorded on the list of card holders so that the access codes can be defined accordingly. Employees with the same access requirements (i.e., the same access code) can be sorted into groups so that their card codes can be entered during database setup with the GROUP command.

In the stand-alone mode, the Alto 818 can retain in memory up to 2,000 key codes (for command key or for VIP2-only codes) by name and number, or 5,200 key codes by number only. It is possible to mix key codes with names and key codes without names. The following formula is used for this purpose: 13 times the number of key codes with a name, plus 5 times the number of key codes without names, must be equal or less than 56,000. For example: assume that 1,465 employees are to be assigned keys with names and numbers. To determine the number of employees that can be assigned keys without names (X), the formula is applied as follows:

$$\begin{aligned}(13 \times 1,465) + (5 \times X) &= 56,000 \\ 19,045 + 5X &= 56,000 \\ 5X &= 36,955 \\ X &= 7,391\end{aligned}$$

Therefore, when 1,465 employees are assigned key codes with both numbers and names, an additional 7,391 employees can be assigned key codes with numbers only.

A complete list of card holders should include the following six elements:

- Key code.
- Card holder name (12 characters maximum).
- Access code.
- Is the card holder to be privileged, granted access to a station reader for the purpose of changing building modes?
- Is a key trace report to be generated each time the card holder presents the card to a reader?
- Is the location to be reported each time the card holder presents the card to a reader?

CARD HOLDER NAMES

Card holder names cannot be longer than 12 characters and each must be unique. An individual can be assigned more than one key code, but the name must be entered in the same manner for each assigned key.

ACCESS CODES

The setup sheets in Appendix B for the access command should be filled out before specific access code numbers can be assigned to individual card holders. Only one access code can be assigned to each key code. Then, after the database is set up and the system is placed in operation, the Alto 818 will grant access to a door only on the days and at the times specified in the access code assigned to the individual's key code.

7.2.4 LISTING ACCESS CODES

Using the list of card holders, the access codes can be defined. After the list of card holders is compiled, the individual card holders can be sorted into groups with the same access requirements. Typical groups might be: Regular employees, janitorial personnel, company executives, maintenance workers, and security guards. Each card holder group can then be assigned a different access code. A maximum of 120 access codes can be set up and assigned on the Alto 818 system.

7.2.5 REPORTS

Reports perform two functions. They provide a record of log events and can be used to initiate system actions.

LOG EVENTS

There are a total of 18 activities which can be assigned a report number: Thirteen with the DOOR command, one with the MONITOR command, and four with the SYSTEM command. These are shown in Table 6-1.

Table 7-1: Selectable Reports

Command	Report Activity
SYSTEM	Duress
	Operator Override
	Power Failure
	Tamper
MONITOR	Monitor Point Active
DOOR	Access Denied
	Access Granted
	Coax Failure
	Device Tamper
	Door Forced Open
	Door Open Too Long
	Exit Denied
	Exit Granted
	Key Trace
	MSM Failure
	Sensor Fail
	S-Net Reader Failure
	VIP Failure

To define reports and assign report numbers, proceed as follows:

1. Make a list of the log events to be reported.
2. For each log event on the list, make a note of the actions that are to be taken each time the log event occurs. Also note the building modes and/or time intervals in which these actions are to be operative.
3. Make a survey of this list and sort the log events that require the same report actions during the same building modes and/or time intervals into separate groups. Assign a report number for each group and enter these report parameters on the setup sheets.
4. During database setup, as the DOOR , MONITOR and SYSTEM commands are used, refer to the setup sheets and enter the assigned report number into the appropriate data fields.

An example of log events which might require the same report actions and therefore use the same report number are hardware failures: Power fail, reader fail, VIP failure, etc. Similarly, most doors will require a report for access granted, access denied and key trace during the same time intervals. Again, one report number can be assigned for all controlled doors for these log events.

REPORT ACTIONS

Each report is set up in the database using the REPORT command, and a specific set of report actions is assigned that defines how the system will respond when a given log event action occurs. For each report assigned a number, the following five report actions must be defined:

- SEND TO HOST
- CLOSE LATCHED CONTACT
- CLOSE CONTACT (0-16)
- PREVENT BUILDING CLOSURE
- PRINT*

1. SEND TO HOST. Is the report to be sent to the host? If so, during which building modes and what time intervals (3 are available)? If a Y is entered for all three building modes for a given report, that report will be sent to the host port 24 hours a day, 7 days a week, including holidays.
2. CLOSE LATCHED CONTACT. Is a latched contact on an SE 778A to be closed when this log event occurs? If so, during which building modes and what time intervals (3 are available)?

This report action is enabled for log event activities that require operator acknowledgment of an abnormal condition. Once closed, the latched contacts can only be opened again by a system operator assigned to rank A through E with the use of the SILENCE command, even though the abnormal condition may have been rectified. (System reset or power failure will also open the latched contacts.) An audible device is typically connected to the latched contacts. Thus an operator is not required to visually observe the log event triggered by the abnormal condition. The operator, however, must acknowledge it to silence the audible device.

When is this report action to be enabled, during which building modes and what time intervals
If a Y is entered for all three building modes, the report will be sent to the host port 24 hours a day, 7 days a week, including holidays. Entering an N for all three building modes and no time intervals, will omit this report action.

3. CLOSE CONTACT (0-16). This report action makes use of eight relay outputs on the Alto 818 (1-8) and the eight relays on the SE 778A (9-16). If 0 is entered in this field, no contacts will close.

A contact closed by a report will open again automatically when the monitored condition is either rectified or an operator with rank A, B, or C evokes the SHUNT.

4. PREVENT BUILDING CLOSURE. Should this report prevent the building from being closed? When some log event activities occur, closing the building during the time of the occurrence could compromise security if this function is not enabled.

Example: A monitor point is connected to a set of contacts that close when a window into the controlled area is opened. Entering Y to this action would prevent the building from being closed if the window was open. If Y is entered for report action 4, Y is usually entered for report action 5, below.

5. PRINT *. Should the report printout be preceded by an asterisk? If Y is entered for this report action, an asterisk will precede the report on the printout, thus flagging the report of a monitored condition or any other exception that requires attention. This will also initiate a modem call if the system is appropriately configured.

7.2.6 LIST OF DOORS

The DOOR command prompts for more than 20 different data entries for each controlled door in the system. In addition, some entries relate to entries in other commands. It is, therefore, particularly important that the database setup sheets be filled out and used when defining the doors.

7.3 CREATING THE DATABASE

Once all the database parameters have been defined, begin entering data into the Alto 818.

7.3.1 ENTERING THE COMMAND MODE

With a terminal connected to the Alto 818, type the user 1 password NEW and press ENTER. If the USER command has already be used to modify the database, the password for a user with rank A must be entered. When a valid password has been entered the screen will display:

```
HELLO USER 1  
TYPE HELP FOR A LIST OF COMMANDS
```

Begin entering database information in the command sequence recommended in section 7.3.3.

Due to tests which may be performed on the Alto 818 controller prior to installation at a site, it is recommended that memory be erased prior to beginning database set up. The test diagnostic TEST2 will erase all database memory.

CAUTION:

Use of the TEST2 command will erase all database memory and return all parameters to the system default values.

7.3.2 EXITING THE COMMAND MODE

Use the command BYE to exit from the command mode. If there is no keyboard activity on the terminal for 4 minutes, the Alto 818 will automatically log out the user and revert to operate mode.

7.3.3 COMMAND SEQUENCE

Once all the required information has been entered on the database setup sheets, the recommended command sequence for establishing a new database in the Alto 818 is:

- | | |
|------------|------------|
| 1. TIME | 7. ACCESS |
| 2. USER | 8. HOLIDAY |
| 3. SYSTEM | 9. KEY |
| 4. REPORT | 10. GROUP |
| 5. DOOR | 11. MODEM |
| 6. MONITOR | |

7.3.4 PRINT COMMAND

Use the PRINT command to verify the data entered.

SECTION 8: OPERATION

This section details the use of commands, described in Section 6, for the operation of the Alto 818. The availability of a particular command depends on the operator's authorization rank (see Table 6-2).

8.1 OVERVIEW

An Alto 818 system requires procedures for initial power on and for terminal setup so that the database can be installed. Once this is accomplished and the system installation is completed, system power should remain on for an extended length of time as security can be compromised if the system is not in operation.

NOTE:

WSE strongly recommends that once the Alto 818 system is up and running and the database setup is completed, an IBM PC-compatible computer be connected and the database be saved to a hard drive or a diskette. This process is accomplished using modem software installed on the PC and the XSAVE command (see Section 6.3.28).

Normal system operation takes place in the operate mode. In this mode, system operators monitor the terminal screen and printer for system activity that may require attention. When no operator is present, abnormal system activity can cause an audible alarm to sound, can cause a dial-up modem to summon help, or can send a report to a remote terminal site.

If operator intervention is required, the operator enters the command mode to change building modes, to add or delete keys, to respond to alarms, etc.

8.2 INITIAL POWER-ON

NOTE:

The initial power-on procedure should be performed by a technically-qualified operator.

Perform initial power-on as follows:

1. With the power switch in the OFF position, connect the power module to the AC source and to the ACU as described in Section 4.1.
2. With the power switch in the OFF position, connect the terminal to ACU as described in Section 4.7.
3. Loosen the six captive screws that attach the cover to the ACU and remove cover.
4. Locate the battery switch (S2) and turn switch to the ON position (see Figure 2-3); replace the ACU cover.
5. Turn the power module ON. At the ACU, the vital function green LED should be blinking; the terminal RX and TX green LEDs and the host TX green LED should be ON.
6. Turn the terminal ON; ignore the screen display and proceed to terminal setup in the following section.

8.3 TERMINAL SET-UP

The following procedure for setting terminal communication parameters applies to the Qume QVT 100+ terminal. However, almost any ANSI terminal can be used to configure the Alto 818 (refer to the individual manufacturers' user manuals for terminal setup procedures).

The Alto 818 is shipped with the terminal port set at 300 baud. The baud rate may be changed to 1200, 2400, 4800, or 9600 as appropriate. A terminal used with the Alto 818 should be set for odd parity, 7 data bits, and 1 stop bit.

The Qume QVT 100+ (or equivalent) terminal is set up using the following procedures.

1. Simultaneously press SHIFT and SETUP keys. Setup menu displays at foot of screen. Scroll down menus to **SET 4 EIA=HOST** using down arrow key. Scroll across this menu using right arrow key. Using space bar to alter settings, set parameters to read as follows:

```
SET 4|EIA=HOST|7 BITS|BIT 8 1|PARITY ON|PARITY ODD|STOP 1|BAUD:
300
```

After all settings are correct, press SETUP key to exit the setup mode.

2. Locate and press the reset switch (S1) (see Figure 2-3) on the ACU; a sample screen display follows:

```
MON 05-JUN-95
```

The date display is followed by log 01 giving the time and the reset message, log 02 with the tamper message, and log 03 with the power fail message. For example:

```
01 02:24:44 RESET
02 02:24:50 TAMPER
03 02:24:50 POWER FAIL
```

If any system faults are detected, log 03 will be followed by further data log entries which report failures. Each failure report will be preceded by a number that denotes the sensor port from which the fault was detected. For example:

```
04 02:24:55 (4) MSM FAIL
05 02:24:57 (1) VIP TAMPER
```

Log 04 indicates a failure of the MSM connected at sensor port 4; log 05 indicates the tamper switch on door 1 VIP is active. If no system faults are indicated, the system is ready to log on and set up the database.

8.4 INITIAL LOG ON

Until a system database has been initially set up, no passwords will have been assigned. The password NEW, however, is preprogrammed at the factory and can be used to permit logging on for database setup purposes. To log on to a system before initial database setup, proceed as follows:

1. After the Alto 818 power module and terminal have been turned on (Sections 8.2 and 8.3), press Enter or the space bar to enter the command mode.
2. The screen displays:

YOUR PASSWORD?

Type NEW and press Enter. If 10 seconds elapse without a password being entered, the screen displays:

TIMEOUT

Press Enter or the space bar to display the password prompt again.

YOUR PASSWORD?

3. After NEW has been properly entered, the screen displays:

**HELLO
TYPE HELP FOR A LIST OF COMMANDS
YOUR COMMAND?**

This display indicates that the operator has been logged on. The system is now ready to accept commands.

8.5 OPERATE MODE

After power-on, the system automatically comes up in the operate mode. In this mode, data logs of system activity are sent to the terminal. An operator can be assigned to the terminal site to watch for reports which will appear on the terminal. In this instance, the operator's functions are passive, observing system activity only. System operation cannot be altered except to change the building mode at a remote L/C station. If operator intervention is required for any reason, the operator must first place the system in the command mode by entering a valid password.

8.6 OPERATOR RESPONSIBILITIES

During normal operation, the Alto 818 does not require operator intervention.

8.6.1 SYSTEM MONITORING

A terminal may be interfaced to the Alto 818 to display all system activity. With an ACU connection to a host, displayed information is selectable through host programming. Figure 8-1 shows an example of the log events displayed on a terminal during one hour of operation. The system must be in the operate mode to display the log events reported to the terminal.

```

WED 07-JAN-98
01 14:07 LOBBY (1) ACCESS GRANTED SMITH, J. (12345)
02 14:08 LOBBY (1) KEY TRACE SMITH, J. (12345)
03 14:11 CAFETERIA (2) REQUEST TO EXIT
*04 14:12 CAFETERIA (2) DOOR OPEN TOO LONG
05 14:14 CAFETERIA (2) DOOR CLOSED
06 14:17 FIRE (3.4) MONITOR POINT ACTIVE
07 14:19 FIRE (3.4) MONITOR POINT CLEAR
08 14:19 REAR (7) ACCESS GRANTED JONES, L (32456)
09 14:23 REAR (7) ACCESS GRANTED BROWN, N (54632)
10 14:24 LOBBY (1) ACCESS GRANTED GREEN, S (14352)
*11 14:27 WEST (5) SENSOR FAIL
12 14:32 WEST (5) SENSOR OK
13 14:33 LOBBY (1) ACCESS GRANTED WHITE, M. (21354)
14 14:33 LOBBY (1) KEY TRACE WHITE, M. (21354)
15 14:42 EAST (2) MANUAL UNLOCK ADAMS, Q (1)
16 14:42 EAST (2) MANUAL RELOCK ADAMS, Q (1)
17 14:45 LOBBY (1) EXIT GRANTED
18 14:45 WEST (5) EXIT GRANTED
19 14:48 LOBBY (1) EXIT GRANTED
20 14:53 LOBBY (1) EXIT GRANTED
21 14:54 REAR (7) EXIT GRANTED
22 14:55 REAR (7) EXIT GRANTED
23 14:57 REAR (7) ACCESS GRANTED WILSON, B (52721)
24 14:57 LOBBY (1) EXIT GRANTED
27 15:06 BLDG CLOSED
  
```

Figure 8-1: Terminal Display Example

8.6.2 RESPONSE TO ALARMS

The Alto 818 can indicate an activity which requires operator intervention through the use of an audible alarm or through a printed report. These parameters are set with the REPORT command, Section 6.3.16. The use of the STATUS command may be needed to determine the cause of the alarm or report generation.

An audible alarm, triggered by the latched contact on an Annunciator, will require that the condition be corrected or the monitor point shunted, followed by the use of the SILENCE command described in Section 6.3.27.

8.7 OPERATION COMMANDS

Eight commands, called direct, are used to override but not reconfigure the system. These commands are CLOSE, LIMIT, OPEN, RELOCK, SHUNT, SILENCE, UNLOCK, and UNSHUNT. When these commands are invoked, an OPERATOR OVERRIDE log message is generated.

If power to the Alto 818 is disrupted, or if the system is reset, the ACU will cancel these direct commands. Only program command data (i.e., the database) is retained in memory when power is restored.

8.7.1 CLOSE

This is an operator override command which manually changes the building mode to closed. When this command is entered, the system first enters the limited mode for one minute before going to closed mode. The mode can be changed again with another operator command.

8.7.2 FORGIVE

Use the FORGIVE command to manually reset all key holder locations to unknown. The location will change when the key holders next access an exit or entrance. The command is required only if anti-passback has been enabled.

8.7.3 LIMIT

This operator override command is used to manually change the building mode to limited. Using this command, the building will remain in limited mode until another operator override command is entered.

8.7.4 OPEN

This command manually changes the building mode to open. The mode can be changed again with another operator command.

8.7.5 RELOCK

The RELOCK command is used to manually relock a door following the use of the UNLOCK command or during an auto-unlock period.

8.7.6 SHUNT

The SHUNT command is used to temporarily turn off a specific access control or alarm monitoring function while the rest of the system is under normal operation. All activities associated with the shunted devices are temporarily disabled.

8.7.7 SILENCE

The SILENCE command causes the latched contact on an SE 778A to be opened. This latched contact is intended for use by an audible alarm. In addition to clearing or shunting the condition which generated the report and latched the contact, the alarm must be unlatched in one of three manners: Resetting the ACU, turning the ACU off, or using the SILENCE command. During normal operation, the SILENCE command is used.

8.7.8 STATUS

The STATUS command can be very important when monitoring system activities or when responding to an alarm. See the STATUS command description in Section 6.3.20.

8.7.9 UNLOCK

The UNLOCK command may be used to manually unlock a door controlled by the Alto 818. This is an operator override command which will remain in effect until the RELOCK command is used, the Alto 818 is reset, the next auto-unlock expires or there is a power failure.

8.7.10 UNSHUNT

Use the UNSHUNT command to resume normal operation of a device disabled with the SHUNT command as described above.

SECTION 9: ANNUAL TEST FOR UL 294 SYSTEMS

After a UL 294 approved system is installed, and annually thereafter, the following system test must be conducted to ensure proper operation. The STATUS and REPORT commands will be useful in verifying system operation.

To perform the SE 818SC annual system test, proceed as follows:

1. Visual Inspection

Inspect all connectors, wiring, and cables on all devices in the system for looseness, damage, or wear; replace as required.

2. AC Input Power Check

Measure the AC input power and verify it is within 10% of the specified rating for the power supply.

3. DC Power Check

Check the S-Net DC power at the supply.

With all network devices operating, check for adequate voltage at each device.

4. Battery Check

Inspect backup battery for cracks, warping, corrosion, etc.; replace if damaged.

With AC power applied to the power supply and the power supply turned on, measure the voltage at the backup battery between TP4 (ground) and the + terminal to verify that it is between 24 and 28 VDC.

Disconnect AC power to power supply and verify that system is still operational. Check only the portions of the system that are powered from the backup battery. Restore AC power to power supply. The battery voltage should not drop below 24 VDC.

5. SE 818SC ACU Check

Verify operation of all LEDs on the front panel.

Visually check all fuses.

Check the voltage of the lithium battery on the PCA. If the voltage is less than 2.8 VDC, replace the battery. Dispose of the old battery in an approved manner.

6. Door Hardware Check

Inspect door switches for damage; replace as required.

Inspect door locks and hardware; replace as required.

Using the system wiring diagram, installation plan and building specifications, verify the operation of all REX and door switches. This may be facilitated by the use of the REPORT and STATUS commands available with a terminal connected to the terminal port (P2) of the ACU. Make repairs as required.

Inspect all sensors, readers and keypads. Verify correct operation.

7. Alarm Condition Check

Verify reporting of alarm conditions as defined in the database and listed in the setup sheets by creating the alarm condition (e.g., holding a door open too long, causing an anti-passback violation, setting off a motion detector, etc.). Use the STATUS command to check alarm status.

8. SE 774A MSM Check

Verify that all inputs are terminated with a 36K-ohm resistor.

Verify correct functioning of each monitor input; short contact pairs and verify state change. Read the contact state with the STATUS command.

9. SE 778 Annunciator Check

Verify the proper operation of LED indicators and fuses on the SE 778.

Verify proper operation of all relay outputs as defined in system database.

APPENDIX A: SPECIFICATIONS

A.1 REGULATORY CERTIFICATION

Class B digital device, Part 15 of the FCC Rules

UL 294 listed access control unit

Emissions – EN50081-2, EN55022, EN60555-2, -3

Immunity – EN50082-1, EN50093, IEC 801-2, -3, -4, -5

CE

MPT 1339

KEMA certificate No. 39497/CE95-4409

A.2 ENVIRONMENTAL CHARACTERISTICS

Temperature: 20 ° F to 120° F (-7° C to 49° C)

Humidity: 10% to 90% non-condensing

A.3 DIMENSIONS

18 in x 10.5 in x 2.25 in (45.72 cm x 26.67 cm x 6 cm)

A.4 POWER CONSUMPTION

AC current – 150 mA at 16 VAC; 55mA at 25.2 VAC

APPENDIX B: DATABASE SETUP SHEETS

Make the required number of copies of the following setup sheets to assist in defining the database parameters.

ACCESS COMMAND SETUP

Door	Access Code (1-120)								
1	Hours	SUN	MON	TUE	WED	THU	FRI	SAT	HOL
	: to :								
	: to :								
	: to :								
	: to :								
2	Hours	SUN	MON	TUE	WED	THU	FRI	SAT	HOL
	: to :								
	: to :								
	: to :								
	: to :								
3	Hours	SUN	MON	TUE	WED	THU	FRI	SAT	HOL
	: to :								
	: to :								
	: to :								
	: to :								
4	Hours	SUN	MON	TUE	WED	THU	FRI	SAT	HOL
	: to :								
	: to :								
	: to :								
	: to :								

ACCESS COMMAND SETUP - continued

Door	Access Code (1-120)								
5	Hours	SUN	MON	TUE	WED	THU	FRI	SAT	HOL
	: to :								
	: to :								
	: to :								
	: to :								
6	Hours	SUN	MON	TUE	WED	THU	FRI	SAT	HOL
	: to :								
	: to :								
	: to :								
	: to :								
7	Hours	SUN	MON	TUE	WED	THU	FRI	SAT	HOL
	: to :								
	: to :								
	: to :								
	: to :								
8	Hours	SUN	MON	TUE	WED	THU	FRI	SAT	HOL
	: to :								
	: to :								
	: to :								
	: to :								

DOOR SETUP

Door Number(1-8)											
1. Name (24)			2. Key Trace Report (0-32)			3. Access Granted Report (0-32)					
4. Access Denied Report (0-32)			5. Open Too Long Report (0-32)			6. Door Forced Open Report (0-32)					
7. Coax Fail Report (0-32)			8A. Sensor Enable (Y/N)			8B. Sensor Fail Report (0-32)					
8C. S-Net Reader Type (None/DKR/SC R) *			8D. S-Net Reader Fail Report (0-32)			E. Digital Key Read Range (0-255)*					
10. Sensor Type(Normal/Open/Closed/Station)			11. Anti-Passback (Entry/Exit/None)			11A. Anti-Passback Type (Hard/Soft)					
12. Reverse Lock (Y/N)			13. Unlock Time (1-240)			14. Open Too Long Time (1-240)					
15. Door Switch (X.Y)			16. REX Switch (X.Y)			16A. Unlock on REX (Y/N)					
Valid REX			SUN	MON	TUE	WED	THU	FRI	SAT	HOL	
:	—	:									
:	—	:									
:	—	:									
:	—	:									
16C. Exit Granted Report (0-32)			16D. Exit Denied Report (0-32)								
17. Auto Unlock			SUN	MON	TUE	WED	THU	FRI	SAT	HOL	
:	—	:									
:	—	:									
:	—	:									
:	—	:									

continue on next page

* SE 818SC only.

DOOR SETUP - continued

18. Read Key While Door Open (Y/N)			19. VIP Enable (Y/N)				19A. VIP Required When Building is:			
Open (Y/N)			Limited (Y/N)				Closed (Y/N)			
VIP Enable			SUN	MON	TUE	WED	THU	FRI	SAT	HOL
:	—	:								
:	—	:								
:	—	:								
:	—	:								
19B. VIP Fail Report (0-32)			20. Device Tamper Report (0-32)							

HOLIDAY SETUP

Holiday	DD-MMM-YY
1	- -
2	- -
3	- -
4	- -
5	- -
6	- -
7	- -
8	- -
9	- -
10	- -
11	- -
12	- -
13	- -
14	- -
15	- -

Holiday	DD-MMM-YY
16	- -
17	- -
18	- -
19	- -
20	- -
21	- -
22	- -
23	- -
24	- -
25	- -
26	- -
27	- -
28	- -
29	- -
30	- -

KEY HOLDER SETUP

[illegible]

MODEM COMMAND SETUP

1. BLDG ID (72)	
2. TELEPHONE (24)	
3. TRY CALLING (1-10)	
4. CALL BACK (Y/N)	

MONITOR SETUP

1. Monitor Point	Name (24)	Report (0-32)
1.1		
1.2		
1.3		
1.4		
2.1		
2.2		
2.3		
2.4		
3.1		
3.2		
3.3		
3.4		
4.1		
4.2		
4.3		
4.4		

continue on next page

MONITOR SETUP - continued

1. Monitor Point	Name (24)	Report (0-32)
5.1		
5.2		
5.3		
5.4		
6.1		
6.2		
6.3		
6.4		
7.1		
7.2		
7.3		
7.4		
8.1		
8.2		
8.3		
8.4		

REPORT SETUP

Report Number								
1. Send to host when building is :	Open (Y/N)							
	Limited (Y/N)							
	Closed (Y/N)							
and also during hours:	SUN	MON	TUE	WED	THU	FRI	SAT	HOL
: to :								
: to :								
: to :								
: to :								
2. Send to terminal and close latched contact when building is:	Open (Y/N)							
	Limited (Y/N)							
	Closed (Y/N)							
and also during hours:	SUN	MON	TUE	WED	THU	FRI	SAT	HOL
: to :								
: to :								
: to :								
: to :								
3. Send to terminal and close contact when building is:	Contact (0-16)				Open (Y/N)			
	Limited (Y/N)				Closed (Y/N)			
and also during hours:	SUN	MON	TUE	WED	THU	FRI	SAT	HOL
: to :								
: to :								
: to :								
: to :								
4. Prevent building closure (Y/N)				5. Print (*) (Y/N)				

SYSTEM SETUP

1. 1060 Key Type (Y/N)		2. 1050 Key Type (Y/N)	
3. 1040/1030 Key Type (0/1040/1030)			
3A. Facility Code		3B. Alternate Facility Code	
4. Tamper Report (0-32)		5. Power Failure Report (0-32)	
6. Building Should be Closed:	SUN	MON	TUE WED THU FRI SAT HOL
: to :			
: to :			
: to :			
: to :			
7. Building Should be Closed Reminder (0-240 MIN)			
8. Host Baud			
9. Terminal Baud			
10. Operator Override Report (0-32)			
11. Address (0-240)			
12. Host XON/XOFF (Y/N)			
13. Terminal XON/XOFF (Y/N)			
14. Auto Forgive Times and Days	SUN	MON	TUE WED THU FRI SAT HOL
: to :			
: to :			
: to :			
: to :			
15. Reader Disable Time (0-240)			
16. VIP Only Key Digits (4-8)			
17. PIN Digits (4-8)			
18. PIN Seed			
19. Pin Grace Period (10-240)			
20. PIN Retry (0-5)			
21. Duress Enable (Y/N)			
21A. Duress Report (0-32)			
22. Show Key Number for VIP Only Key (Y/N)			

USER SETUP

	1. Name (12)	2. Password (12)	3. Rank (A-F)
User 1			
User 2			
User 3			
User 4			
User 5			
User 6			
User 7			
User 8			

APPENDIX C: COAXIAL CABLE VENDORS

SE 9284 – Standard Coax; WSE Part Number 13100240002

Belden 800	Commscope, Inc. 1375 Lenoir Rhyne Blvd. SE Hickory, NC 28602 (704-324-2200	Southwest Wire and Cable 4320 Yale Blvd. NE Albuquerque, NM 87107 505-344-3400
---------------	---	---

SE 9284PL – Plenum Coax; WSE Part Number 13103437002

Times Fiber Communications 358 Hall Avenue Wallingford, CT 06492 203-265-8500	Commscope, Inc. 1375 Lenoir Rhyne Blvd. SE Hickory, NC 28602 704-324-2200	Southwest Wire and Cable 4320 Yale Blvd. NE Albuquerque, NM 87107 505-344-3400
--	--	---

Remee, Inc. Route 17A Florida, NY 10921 914-651-4431	West Penn Wire Corp. 2833 W. Chestnut St. Washington, PA 15301 412-222-7060
---	--

SE 9284DB – Direct Burial Coax; WSE Part Number 13102705002

Commscope, Inc.
1375 Lenoir Rhyne Blvd. SE
Hickory, NC 28602
704-324-2200

SE 9284EL – Elevator Coax; WSE Part Number 13107721001

Times Fiber Communications 358 Hall Avenue Wallingford, CT 06492 203-265-8500	Belden 800-
--	----------------

The following vendors will sell small quantities of cable:

Carolina Cable Connector 8205 Brownleigh Drive Raleigh, NC 28642 918-881-2140	Zack Electronics 2514 Channing Ave. San Jose, CA 95131 408-942-5432
--	--

APPENDIX D: COMMAND KEYS

A brief overview of the analog and digital command keys is given below.

D.1 ANALOG COMMAND KEYS

The Alto 818 will recognize SE 1030, SE 1040, SE 1050 and SE 1060 analog command keys, but 1030 and 1040 keys cannot be mixed. These keys can be identified by the number digits as shown in Figure D-1 and Table D-1. Analog command keys are 3.36 in x 2.125 in x .01 in (8.53 cm x 5.38 cm x 0.25 cm); operating temperature range is -50° F to 120° F (-46° C to 49° C).

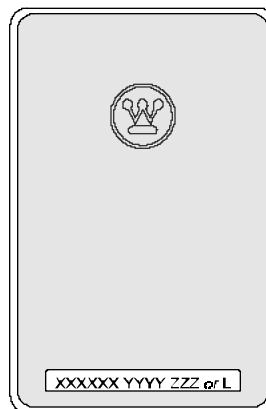


Figure D-1: Analog Command Key Number

Table D-1: Command Key Identification

	Key Number XXX...	Number Range	Facility Code YYY...	Data Code YYY...	Run Code ZZZ	Library Code (Optional)
SE 1030	5-digit	00001 to 999999	4-digit	N/A	3-digit	N/A
SE 1040	6-digit	000001 to 999999	4-digit	N/A	3-digit	N/A
SE 1050	8-digit	00,000,001 to 24,040,016	N/A	7-digit	N/A	1-digit
SE 1060	8-digit	24,040,017 to 60,999,999	N/A	7-digit	N/A	1-digit

D.2 DIGITAL COMMAND KEYS*

All digital command keys, Figure D-2, may be used with the complete DigiReader product line. Specifications for the keys are shown in Table D-2. Table D-3 provides the read range for each type of key. The maximum read range assumes ideal conditions, with no RFI.

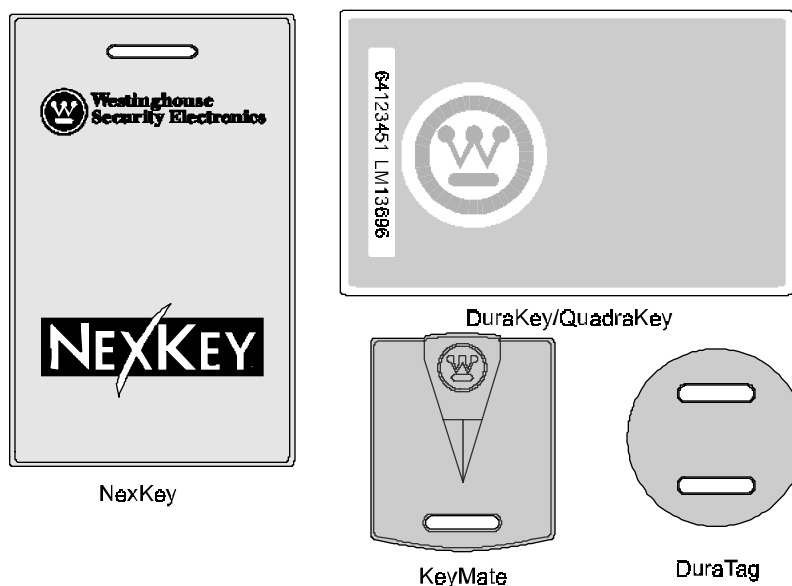


Figure D-2: Digital Command Keys

* Supported by the SE 818SC only.

Table D-2: Digital Command Key Specifications

	Size	Temperature	Humidity	Technologies
QuadraKey	3.37 in x 2.125 in x 0.032 in (8.55 cm x 5.39 cm x 0.081cm)	14° to 140° F (-10° to 60° C)	0 to 100% condensing	• Digital proximity • Magnetic stripe • Photo ID w/ laminate • Bar code • Smart Card chip
NexKey	3.37 in x 2.125 in x 0.035in (8.55 cm x 5.39 cm x 0.19cm)	14° to 140° F (-10° to 60° C)	0 to 100% non-condensing	• Digital proximity • Direct photo ID • Bar code
DuraKey	3.37 in x 2.125 in x 0.099in (8.55 cm x 5.39 cm x 0.025m)	14° to 140° F (-10° to 60° C)	0 to 100% non-condensing	• Digital proximity • Photo ID w/ laminate • Bar code
DuraTag	1.37 in round x 0.192 in (3.45 cm round x 0.484 cm)	-31° to 270° F (-35° to 132° C)	0 to 100% condensing	• Digital proximity
KeyMate	1.375 in x 1.625 in x 0.125 in (3.49 cm x 4.13 cm x 0.32)	-31° to 270° F (-35° to 132° C)	0 to 100% condensing	• Digital proximity

Table D-3: Digital Command Key Read Ranges

	DR 4204	DR 4205/E	DR 4208	DR 4226	DR 4238
QuadraKey	up to 2 in (5 cm)	up to 4 in (10 cm)	up to 7 in (18 cm)	up to 13 in (33 cm)	up to 22 in (56cm)
NexKey	up to 2 in (5 cm)	up to 4 in (10 cm)	up to 7 in (18 cm)	up to 13 in (33 cm)	up to 22 in (56cm)
DuraKey	up to 3 in (8 cm)	up to 6 in (15 cm)	up to 8 in (20 cm)	up to 22 in (56 cm)	up to 36 in (91 cm)
DuraTag	up to 1 in (2.5 cm)	up to 2 in (5 cm)	up to 4 in (10 cm)	up to 10 in (25 cm)	up to 15 in (38 cm)
KeyMate	up to 1 in (2.5 cm)	up to 2 in (5 cm)	up to 6 in (15 cm)	up to 12 in (30 cm)	up to 15 in (38 cm)

Index

Symbols

20mA 2-22, 2-23
connector 2-8
wiring 4-19

A

AC power 4-2
ACCESS 7-4, 7-8, 7-12
access code 6-7, 7-3, 7-5, 7-6, 7-7
access control 1-4
Alarm-Saf 2-13, 4-4–4-6
batteries 2-14
battery 4-4
electrical characteristics 2-13
enclosure 2-15
fuses 2-14, 4-4
LED indicators 2-14
multiple supplies 4-5
Alto 818
battery switch 2-5
connectors, table 2-7
features 1-3
input power 4-2
analog command keys D-1
analog sensor 2-24
models 2-24
test 5-10
annunciator. *See* SE 778-A
anti-passback 1-9, 1-10, 6-12, 6-16
hard 1-9
installation 1-10
soft 1-9, 1-10
authorization rank 6-6, 7-2
auto forgive 6-32
auto unlock 6-14

B

basic functions 2-4
battery
controller 2-5
bench test
equipment required 5-3
procedures 5-6
setup 5-3
building ID 6-21

building mode 1-5, 1-11, 7-6, 7-8, 7-9
changing 1-6
CLOSED 1-6
LIMITED 1-6
OPEN 1-6
BYE 7-11

C

call back 6-22
card holder 1-5
name 7-7
CI-1 2-22
CI-8 2-23
CLOSE 1-6, 7-9, 8-9
closed reader 1-11
coaxial cable
approved vendors C-1
installation 3-10
command
ACCESS 6-7
BYE 6-8
CLOSE 6-8
DELETE 6-9
DOOR 6-9
FORGIVE 6-16
GROUP 6-16
HELP 6-17
HOLIDAY 6-17
KEY 6-18
LIMIT 6-21
MODEM 6-21
MONITOR 6-23
OPEN 6-24
PRINT 6-5
RELOCK 6-24
REPORT 6-24
SHUNT 6-26
SILENCE 6-27
STATUS 6-28
SYSTEM 6-29
TIME 6-34
UNLOCK 6-35
UNSHUNT 6-36
USER 6-36
VERSION 6-37
XLOAD 6-37
XSAVE 6-38

- command key 1-5, 1-10, 6-19, 7-6
 - analog D-1
 - digital D-2
- command mode 2-35
- command type 6-5
- concealed reader 3-7
- connector
 - 20 mA 2-8
 - annunciator 2-9
 - host 2-8
 - power 2-7
 - relays 2-8
 - RS-485 2-9
 - S-Net 2-9
 - sensor 2-9
 - terminal 2-9
- controlled doors 3-18
- controller
 - battery 2-5
 - switches 2-6

D

- database
 - capacity 7-6
 - commands 6-5
 - preparation 7-5
 - setup 7-2
- date entries 6-2
- day entries 6-2
- DC power 4-4
- default 7-3, 7-4
 - parameters 7-3
- DELETE 6-9
- dial-up remote 4-20
- DigiReader 2-27
- digital command keys D-2
- digital reader 2-27, 4-10
 - test 5-11
- DOOR 1-9, 7-7, 7-8, 7-10, 7-12
- door
 - control 1-8
 - lock 1-8, 3-18
 - open too long time 6-13
 - switch 1-9, 3-20, 6-13
 - unmonitored 3-18
- DR 4205K 2-29
- duress
 - code 1-12, 2-29
 - enable 6-34

E

- emergency access 3-2
- Enter key 6-4
- environmental requirements 3-5
- Escape key 6-4

F

- facility code 6-29
- floor plan 3-3
- FORGIVE 1-10, 8-9

G

- grounding 4-2
- GROUP 7-2, 7-6, 7-12

H

- hardware location 3-6
 - Alto 818 3-6, 3-17
 - analog sensors 3-6
 - digital readers 3-8
 - remote station 3-8
- HELP 6-6, 7-11
- HOLIDAY 7-12
- host 2-16
 - baud 6-30
 - connector 2-8
 - port 7-4, 7-9
 - wiring 4-15
- humidity 3-5

I

- initial power-on 8-3
- installation
 - coaxial cable 3-10
 - multiple Alarm-Saf 4-5
 - multiple Power Inserters 4-8
 - planning 3-1, 3-2
 - S-Net devices 4-9
 - sequence 3-21
 - single Alarm-Saf 4-5
 - single Power Inserter 4-7
 - wiring requirements 3-9

K

- KEY 1-5, 1-10, 7-12
- key holder 1-5
- key trace 6-11, 6-17, 6-20
- key type 6-29
- keyboard entries 6-2

L

latched contact 2-18, 4-18
 close 6-25
LED panel 2-6
LIMIT 1-6, 8-9
location 6-17, 6-20
lock
 relay test 5-8
 reverse 6-13
 wiring 4-12
log message 1-6, 1-10, 1-11, 7-4, 7-7, 8-9
log on 8-5

M

manual conventions 1-2
MODEM 7-12
modem 2-30
 short-haul vs. long-haul 2-30
MONITOR 7-7, 7-8, 7-12
monitor point 1-4, 2-20, 3-20
 designator 2-21, 3-20
 test 5-9
 wiring 4-13

N

National Electrical Code ANSI/NFPA70 1-1
NexStar 2-31, 3-14
null modem 4-15

O

OPEN 1-6, 1-9, 8-9, 8-10
open reader 1-7
operate commands 6-5, 8-9
operate mode 2-35, 8-6
operation 8-1
 principles 1-5
operator override 8-9

P

PIN 2-28
 digits 6-33
 grace period 6-33
 retry 6-33
 seed 6-33
power connector 2-7
Power Inserter 2-15
 installation 4-7
 multiple 4-8
 single 4-7
 wiring 4-7

power supply 2-10, 2-12, 3-9, 3-16, 4-4, 4-6, 4-8
power-on 8-3
PRINT 6-5
printer 2-16
privileged 1-7, 1-11, 6-16, 6-20

R

rank 6-6, 7-2, 7-3, 7-9, 7-11
read range 6-12
reader
 disable time 6-32
 type 6-11
relay 1-8, 7-2, 7-4, 7-9
 close 6-26
 connector 2-8
 output 2-18
RELOCK 8-9, 8-10, 8-11
remote station 1-11, 2-19, 3-8
remote terminal
 interface wiring 4-17
REPORT 6-24, 7-12
report
 actions 7-9
 COAX FAIL 6-11
 DEVICE TAMPER 6-15
 DOOR FORCED OPEN 6-11
 DOOR OPEN TOO LONG 6-11
 DURESS 6-34
 EXIT DENIED 6-14
 EXIT GRANTED 6-14
 MSM FAIL 6-12
 OPERATOR OVERRIDE 6-32
 POWER FAIL 6-29
 SENSOR FAIL 6-12
 SNET READER FAIL 6-12
 TAMPER 6-29
 VIP FAILURE 6-15
request-to-exit. See REX
reverse lock 6-13
REX 1-9, 1-10, 3-20
 switch 6-13
 unlock on 6-14
 valid times and days 6-14
RS-232 2-22, 2-23
 wiring 4-15
RS-485
 connector 2-9
 test 5-10
 wiring 4-9, 4-10

S

- S-, E-, and H-mode operation 1-4
- S-Net 2-32
 - address switches 4-10
 - cable 3-13
 - cable losses 3-11
 - devices 4-6, 4-9
 - power 4-4
 - power requirements 3-16
 - termination 3-14
 - test 5-10
 - wire size 3-12, 3-13
- safety 3-2
- SE 2804 2-25
- SE 2814/15 2-24, 2-27
- SE 2854/55 2-25
- SE 3018-2 2-12
- SE 3018S 2-12
- SE 3708C 2-13
- SE 3708CU 2-10, 4-2
- SE 3718SU 2-10, 4-2
- SE 5200 2-30
- SE 6000 4-16
- SE 774-A 2-7, 2-20
 - controller switch 2-7
 - wiring 4-13
- SE 778-A 2-9, 2-17
 - connector 2-9
 - wiring 4-18
- sensor type 1-7
 - closed 1-7
 - normal 1-7
 - open 1-7
 - station 1-7
- show key number 6-34
- SHUNT 7-9, 8-9, 8-10, 8-11
- SILENCE 7-9, 8-8, 8-9, 8-10
- station reader 7-6
- station switch 2-18
- STATUS 8-8, 8-10
- switch
 - controller
 - battery 2-6
 - goof 2-6
 - MSM 2-7
 - reset 2-6
 - door 1-9, 1-10, 2-33
 - REX 1-9, 1-10, 2-33, 2-34, 6-13
 - station 2-18
- SYSTEM 7-7, 7-8, 7-12
- system administrator 7-2

T

- tamper 4-9
- tamper switch 1-11
- telephone number 6-22
- terminal 2-16
 - baud 6-30
 - connector 2-9
 - set-up 8-4
 - wiring 4-15
- termination 3-14
- test
 - analog sensor 5-10
 - DigiReader 5-10, 5-11
 - lock relay 5-8
 - monitor input 5-9
 - RS-485/S-Net 5-10
 - VIP2 5-11
- TIME 7-12
- time entries 6-3

U

- Underwriters Laboratories 1-1
- UNLOCK 8-9, 8-10, 8-11
- unlock
 - on REX 6-13
 - time 6-13
- unmonitored doors 3-18
- unpacking 5-1
- UNSHUNT 8-9, 8-11
- USER 7-2, 7-11, 7-12

V

- VERSION 6-37
- VIP2 2-28
 - enable 6-15
 - LEDs 2-29
 - only digits 6-33
 - stand alone operation 2-29
 - test 5-11

W

- wire insertion 3-15
- wiring requirements 3-9, 4-1

X

- XLOAD 6-37, 7-2
- XON/XOFF
 - host 6-32
 - terminal 6-32
- XSAVE 6-37, 6-38, 7-2